The Defense Science Board Task Force

on

TACTICAL BATTLEFIELD COMMUNICATIONS

Final Report

December 1999

Office of the Under Secretary of Defense
for Acquisition and Technology
Washington, DC 20301-3140

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 1999	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Defense Science Board Task Force on Tactical Battlefield Communications	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Under Secretary of Defense for Acquisition and Technology Washington, DC 20301-3140**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**222**	

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

17 December 1999

Dr. Craig I. Fields
Chairman DSB, OUSD(AT&L)
3140 Defense Pentagon, Room 3D965
Washington, DC 20301-3140

Dear Dr. Fields:

Attached is the final report from the Defense Science Board Task Force on Tactical Battlefield Communications. The Terms of Reference for the study requested that the Task Force assess the Department of Defense's strategies and processes for providing communications infrastructure to support our warfighters' information needs and ultimately for achieving Information Superiority as premised in Joint Vision 2010.

As the Task Force undertook its charge, it decided to review and assess not just Department of Defense issues associated with architecting, procuring, and maintaining an appropriate communication infrastructure for our warfighters, but to do the same for the telecommunications infrastructure that underlies the World Wide Web. This decision was made because of the double-digit growth, year after year, of telecommunications infrastructure, technologies, and capacity that is occurring in the private sector.

Using the Terms of Reference as a guide, parallel assessments for both sectors were made with regard to their respective telecommunications infrastructure: vision, requirements, architectures, existing technologies, acquisition, and strategies, and unique requirements. Our findings indicate that there are strong similarities between the needs, goals, and technologies required by *users* in both sectors. Furthermore, although DoD *had* many unique telecommunications requirements in the past, many of these can now be met with private-sector technologies, architectures, and systems.

Significant differences between the two sectors occur primarily with regard to where telecommunications technology innovation is occurring, and the acquisition strategies and processes for integrating these technologies into an integrated information infrastructure. The private sector has evolved to an architectural framework that results in a flexible, scalable, packet-switched, Quality-of-Service-based, integrated Internet. Facilitated and fueled by the growing e-commerce market, new terrestrial and space-based telecommunication technologies are being rapidly integrated into the Internet.

Although the Department of Defense has modeled and demonstrated in experiments the value of internetworked telecommunications for enhancing military operational capabilities, the Department's ability to transition the private sector's Internet architectural framework and to leverage private-sector telecommunication technologies is hindered by the lack of a Department-wide technical vision, governance body, policy, capstone requirements, and acquisition processes to put in place a secured, Quality-of-Service-based, Department of Defense virtual Intranet—a Global Information Grid.

Based on its findings, the Task Force has formulated a set of eight recommendations that are believed to be fundamental for providing, at reasonable cost, adequate telecommunications infrastructure to meet our projected Department of Defense national security needs. We believe these recommendations are pivotal for delivering to our warfighters a Global Information Grid (integrated information infrastructure) to support their needs for Information Superiority in the next century. These recommendations are discussed in depth in our report, as are the findings that led to their formulation.

I would like to express my sincerest appreciation to the Task Force members and government advisors whose technical and operations insights, hard work, dedication and passion for helping the Department resulted in the Task Force report. I would also like to thank the briefers who presented their views on the issues the Task Force addressed. We hope that our sponsors find the information contained in this report useful and that the specific recommendations we made actionable.

Sincerely,

Michael S. Frankel, Ph.D.

Chairman, DSB Task Force on
Tactical Battlefield Communications

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

At the outset of this study, the Task Force observed that there was no such thing as "just" tactical communications. Rather, it saw requirements for conducting military operations in two major theaters of war as well as for conducting a wide variety of other missions. It also saw emerging requirements for a telecommunication infrastructure to support rapid force projection, early entry, reachback/split-base, and high mobility operations. Furthermore, Joint Vision 2010 (JV2010) assumed information superiority to be necessary for dominant maneuver, precision engagement, full dimensional protection and focused logistics. All these factors have led our Military Services to express a need for a fully integrated, strategic/tactical, voice/data/information telecommunications infrastructure rather than merely "tactical" communications. This infrastructure must bring post-camp-station information services to deployed forces and, conversely, bring information from our deployed forces to the continental United States (CONUS) or to other locations geographically distant from areas of operations.

Although the Task Force expanded its view to go beyond its Terms of Reference (TOR) "Tactical," it also needed to narrow its view somewhat to keep the study manageable. It did this by not considering people issues such as recruitment, training, retention, or skills. Further, it did not consider information services above communications (transport); nor did it consider applications or middleware, all elements of a fully integrated Global Information Grid (GIG). Also not considered were intelligence data transport systems, including emerging Petabit concepts. The Task Force did, however, consider intelligence product dissemination in its deliberations.

This report presents the following in sequence: the structure of the study itself; the Task Force's findings from the private sector—the sector that is driving the information technology and infrastructure, systems revolution; the panel's findings from the Department of Defense (DoD)—the sector that in the past, but no longer, drove information technology; panel recommendations for establishing the needed telecommunications capabilities for the DoD; and finally its overall conclusions.

STRUCTURE OF THE STUDY

The Terms of Reference for this study asked the Task Force to determine the adequacy of: the forecasted DoD Joint Tactical communication requirements; DoD communication vision and architecture to meet these requirements; DoD communication security architecture; existing communication resources to meet forecasted requirements, funding, and capitalization constraints that impede achieving the vision and meeting the requirements; and acquisition strategy and policy to meet requirements through exploitation of commercial and DoD-unique communication technologies. The Task Force was asked to make recommendations based on its findings.

The study was co-sponsored by the following persons: the Honorable Dr. Jacques Gansler, Under Secretary of Defense for Acquisition, Technology and Logistics (USD/AT&L); the Honorable Art Money, Assistant Secretary of Defense for Command, Control, Communications,

and Intelligence (ASD/C3I); and LTG John Woodward, J6. The Task Force comprised fourteen experts from government, industry, and academe. The Executive Secretaries were Mr. Bennett Hart and Mr. Vic Russell, both from the Office of the ASD/C3I. Government advisors from J6, Army, and Air Force* were chosen to assist the Task Force and to ensure that views from the stakeholder DoD organizations were considered in the study and that deliberations of the panel were discussed within the advisors' parent organizations.

The Task Force began its information gathering in November 1998 and subsequently held two-day meetings on a monthly basis through November 1999. Over 70 briefings were presented by individuals representing a similar number of organizations in both the public and private sectors. Each session provided both information gathering and debate opportunities. This information, the discussions, and the expertise of the Task Force members provided a strong basis for the findings and recommendations presented in this report.

FINDINGS—PRIVATE SECTOR

The requirements in the private sector are market-based. The engines powering the rapid growth in Internet subscribers (171 million worldwide) and Internet host sites (40 million) are e-commerce, both individual and business-to-business, as well as the delivery of Internet services including the rapidly emerging Voice over the Internet Protocol (VoIP). Both fiber optic systems and commercial satellite services are projected to continue to grow rapidly to address this expanding demand for e-commerce and converged multimedia services.

The private sector has evolved a clear and implementable vision for the future of data and voice telecommunications. That vision posits that information is a valuable commodity that must be available when and where needed; that everyone and everything will be part of the "Web"; that entities integrated into the Web will be static/mobile, people/sensors, and sources/users; and that the infrastructure will be scaleable, flexible, and adaptable. The architecture is the Internet, a standards-based, integrated network-of-networks. It is a common-user, and will be a quality-of-service (QoS)–based, infrastructure with services provided over a common, open protocol called the Internet Protocol (IP). Many types of media are integrated into the Internet, including fiber optics, space-based telecommunications to extend/bypass the fiber medium, and land-based wireless technology to support mobile users. This architecture is converging to an integrated infrastructure where the convergence layer is IP. This protocol is based on packet-switching transport, has worldwide acceptance and use, and provides common-user, integrated services with QoS being rapidly implemented. It provides a standardized interface between information application and transport services.

The convergence to IP as the means of integrating multiple disparate networks into a network of networks and its use to support multiple types of services such as voice, video, and data (multimedia), is a radical departure from the architecture and technology that has existed in the past. The private sector's circuit-switched infrastructure, an end-to-end, preallocated, and dedicated bandwidth architectural framework, is rapidly being replaced by the Internet's common-user, shared media architectural framework. This shared medium (typically represented

*Navy participation was sought but not provided.

as a “cloud”) allows for dynamic resource allocation, (e.g., bandwidth), minimizes waste of preallocated but unused resources, and allows the infrastructure to easily and efficiently grow as demand dictates. The sharing and dynamic allocation of resources, to be based on QoS, reduces the costs of use and ownership. Furthermore, the fact that all users share a common infrastructure and common addressing and naming conventions means that any user(s) can send information to any other user(s). This degree of functional flexibility is not easily supported in the earlier circuit-based point-to-point framework.

The expansion of the Internet has fueled and has been facilitated by the availability of broadband transport links between the network and internetwork packet switches. Two specific media are rapidly growing—ground-based fiber optics and space-based satellite data communications.

Fiber optic networks have become the backbone of the Internet. These systems have migrated from point-to-point links to a network model that can handle VoIP and machine-to-machine data exchange. Network capacity is growing over existing and new fiber-optic media as a result of technology breakthroughs such as Dense Wave Division Multiplexing (DWDM). “Carrier sovereignty” is now achieved through wavelength “ownership,” as opposed to cable ownership. Techniques to permit add and drop capability at shoreline or submerged multiplexers are available, and bandwidths of over 100 Gbps have been demonstrated over transoceanic distances. Total transoceanic capacity is expected to grow by more than an order of magnitude to over 10,000 Gbps by 2004. The installation of this capacity, along with the attendant intracontinental capacity, will ensure the fiber availability of fiber-optic networks in littoral and inland areas worldwide.

Today the mobile Internet user is supported worldwide by ground-based personal communications systems (PCSs) and in the near future will be supported by a broad spectrum of different types of commercial satellite communications systems. These systems will include relatively sparsely deployed geostationary orbit (GEO) systems and highly proliferated low earth orbit (LEO) constellations. Such systems will support an equally broad range of voice/data services ranging from narrow-to medium-bandwidth mobile information services to broadband fixed-site services. These systems will be integrated into the Internet and become another transport medium supporting multimedia applications. It is interesting to note that former DoD personnel are playing an active role in the development of commercial satellite systems.

The private sector is accelerating its development of security technology to protect e-commerce growth on the Internet. These security technologies will provide information assurance (IA) between multimedia applications and people who exchange information across the many different types of networks that comprise the Internet. Again, it is e-commerce that is driving commercial security standards, architectures, and technology. There is strong industry motivation to provide privacy, authentication, integrity, continuity of service, verification, and nonrepudiation. Many of these IA services are being supported through public key infrastructure (PKI) technology that is rapidly maturing and being deployed rapidly. Furthermore, PKI, integrated with database systems and Intrusion Detection Systems (IDSs) is being used as a mechanism to reduce the insider threat in the private sector. Importantly, in this technology area there is also a knowledgeable workforce having significant prior DoD security experience.

Security technologies are readily available, a standards-based architecture is being promoted, and the concept of multiple levels of security (vs. multiple-level security) is being supported in the private sector. The need for a formal security framework addressing policy and process, communication, training, and technology is accepted, and security is gathering acceptance and is now viewed as a management responsibility. The Internet community security requirements have matured to where they are becoming parallel to those of the DoD.

All commercial information infrastructure technologies that are being developed are acquired and integrated with a requirement that they be continuously refreshed. For example, commercial satellite system planners expect to recapitalize the commercial space-based infrastructure every five to eight years. For ubiquitous fiber-optic systems, continuous upgrade of the switching infrastructure is necessary to meet demand; one network provider is currently investing $3,000,000 per day to upgrade its switches. The end-user information technology (IT) devices are made simple and inexpensive; their expected lifetime is 2 to 3 years or less, after which they are discarded.

In summary, the private-sector *customer* demands and gets, over time and through market competition, more and better information and communication services for less cost and risk. The private sector telecommunications infrastructure, technology and systems are growing in capability at double-digit rates year by year; this growth is facilitated by a common architectural framework that permits new technologies and systems to be easily and efficiently integrated into the Internet. The diversity of services supported over the Internet is growing rapidly and ranges from voice, video, and data services to hand-held devices as well as to desktop computers. All the while, the costs of services and technology are consistently decreasing.

FINDINGS—DOD

Through extensive fact-finding efforts, the Task Force ascertained that there is no established and accepted DoD database of Joint Information Exchange Requirements (JIERs). While there are several studies that demonstrate where joint connectivity is needed for Joint Task Force (JTF) operations, these studies have not resulted in quantified requirements accepted by the DoD community. Nonetheless, the Joint Chiefs of Staff (JCS) J6 is developing a communication modeling and simulation system called Network Warfare Simulation (NETWARS). The Task Force noted the importance of NETWARS to DoD and the significant progress made by this program. This system will be an effective tool to assist DoD in making telecommunication technology acquisition tradeoffs and decisions. It will, however, require a set of validated JIERs for a spectrum of JTF force structures and missions in order to be effectively used. The NETWARS program is seeking to develop such a database.

Similarly, discussions with the Commanders in Chief (CINCs) did not lead to the discovery of quantified and verified JIERs. The CINCs accept the JV 2010 Information Superiority premise, and they noted that JIERs are JTF dependent—each JTF is different and dynamic in structure. They also noted that interoperability between and among Service command and control (C2) systems is difficult, and Service communication systems must be patched together on a case-by-case basis. The inclusion of coalition partners only complicates this situation further. The CINCs have expressed future JTF communications requirements in subjective

(interoperable, flexible, survivable, affordable. . .) or broad (same capabilities "in the field" as at headquarters) terms. It is interesting to note that these are the same terms used by private sector customers when addressing their information and telecommunication needs.

Task Force discussions with the Services led only to quantified requirements at the Service operations level. These requirements were based on prior experiences and perceived, but unsubstantiated needs for the future. The Service representatives acknowledged that they would operate jointly, but provided no requirements for joint communications capacity and links. They capture only Service communication requirements in their IER databases.

Because of the lack of information on JIERs, the Task Force derived a conservative estimate for the peak total capacity required for two Major Theaters of War (MTW). Its analysis resulted in an estimate for 2010 of 35 Gbps—almost 20 times what was used in the (uncontested) Bosnia operation in 1997. This estimate was based on extrapolations of results from a recent Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Mission Assessment (CMA) Study (1997). The DSB Task Force estimate was then benchmarked against several real-world experiences to establish and support its reasonableness.

Major capacity drivers in the estimate were imagery, video, computers, and telephones; should logistics and medical JIERs be included, the estimate would be many times larger. Furthermore, experience with the Internet in the private sector has shown that capacity requirements grow as on-line organizations reengineer their business processes to take advantage of the interconnectivity between themselves and the rest of the Internet community. One example of such process reengineering in DoD is a concept called Cooperative Engagement Capability (CEC). CEC and others will emerge as our DoD forces, weapons and people are integrated through broadband telecommunications. These "process" reengineering concepts for achieving greater military effectiveness will cause a surge in capacity requirements if the private sector analogy holds true. Even if this surge does not occur, the Task Force noted that its 2 MTW estimated peak capacity (telecommunications requirements) far exceeds the total capacities of current and planned DoD communication systems, even when projected over the next decade.

Other factors complicate DoD's ability to meet future joint telecommunication requirements. First, there are complicated spectrum allocation issues including politics, policy, processes, and efficient use. Second, there are Title 10 arguments about who is in charge. Finally, and perhaps most importantly, there is a significant lack of "systems" perspective and independent system engineering organizations within DoD to provide the necessary studies and analyses. There is a scarcity of the people, resources, understanding, tools, and independence needed to openly address the shortfall in meeting DoD's present and future telecommunication requirements through DoD's planned system acquisition strategies.

The lack of Joint requirements and the aforementioned complicating factors are exacerbated by the fact that the DoD has not yet promulgated a vision specific enough to develop an implementation plan for an integrated Joint telecommunications infrastructure. DoD's JV2010 premise of information superiority has been accepted by the CINCs and the Services and acknowledged to be critical to the success of future military operations. However, JV2010 provides no insight as to how information superiority will be achieved. Network-Centric

Warfare (NCW) adds some technical depth to JV 2010, points to information technology experience in the private sector, and attempts to help DoD and the Services understand and accept the value of a shared, common-user digital communication environment. However, NCW is also too general to allow a DoD implementation strategy and plan to be set for the infrastructure.

Despite the absence of a sufficiently specific "vision" and concomitant implementation plan, numerous concepts for achieving information superiority are emerging from various communities. Examples of these concepts include the Global Information Grid (GIG), (Office of the Secretary of Defense [OSD/J6]), the Global Grid, (Air Force [AF]), the Global Grid, (National Reconnaissance Office [NRO]), Infosphere, (Air Force Science Advisory Board [AFSAB]), the Integrated Information Infrastructure (Defense Science Board [DSB]), the Tactical Internet (Army), the Naval Command Information Infrastructure, (Naval Studies Board [NSB]), and the Global Grid Architecture, (Federally Funded Research and Development Center [FFRDC]). These concepts are attempting to add process, policy, requirements, or technical depth (from a Service or OSD perspective) to JV2010 and NCW.

A specific example of a DoD initiative that has been attempting to establish policy, process and strategy for a DoD "enterprise" information infrastructure is the Global Networked Information Enterprise (GNIE). This initiative was, however, not focused on developing a DoD-wide information infrastructure system architecture that integrated the tactical through strategic telecommunication resources. Rather, it was focused on establishing a process to define and develop a DoD-wide infrastructure focused on enterprise business operations. It delegated to the Services the acquisition of information technology to meet warfighter operational information infrastructure needs.

From each component Service perspective, future war fighting concepts of operations are also evolving, and such concepts place greater demands for communication capabilities. Examples of future concepts of operation include the Air Expeditionary Force (AEF), the Army 2010 and Beyond, Operational Maneuver from the Sea (OMFTS), and Navy Forward From the Sea. Such concepts of operation hypothesize a telecommunication infrastructure that has flexible capacity (bandwidth on demand), does not encumber force mobility (wireless), is easily deployable (light, small), is self-organizing, has global coverage (reachback), provides integrated services (voice, video, data), is secure and survivable, and provides assured access to the warfighter. Unfortunately, despite this desire for our integrated information infrastructure to achieve information superiority in an extremely dynamic military operational environment, there is no accepted detailed vision, governance body, reference model, implementation plan, system architecture, and roadmap for a joint integrated transport infrastructure or Global Information Grid. Such a body is needed to set acquisition policy, establish acquisition plans, set investment priorities, focus Service communication initiatives, exploit emerging technologies/infrastructure, and, in the end, meet the users' needs.

However, the DoD does have an architectural framework consisting of the Operational Architecture (OA), the System Architecture (SA), and the Technical Architecture (TA) that is widely accepted and could be the foundation for the GIG. An Architecture Coordination Council (ACC) has been established to manage the development and evolution of the three architectures.

The J6 has been tasked to develop the Joint Operational Architecture (JOA), which should be viewed as a set of OAs that span the spectrum of JTFs and the missions they will support. These JOAs will be critical for defining JIERs. The ASD/C3I has been tasked to develop the Joint System Architecture (JSA) and the Joint Technical Architecture (JTA). The JTA, whose primary goals are to insure and facilitate command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) system interoperability and to help DoD exploit commercial information technology, is a standards-based architecture incorporating both DoD and commercial standards. The primary goal of the JTA, however, is currently being put in jeopardy by the consensus-based management philosophy used to select standards for incorporation into the architecture—the number of standards is growing with time, in part due to the growing number of information standards embodied in Internet technologies, but also due to the attempt to incorporate legacy and favored standards from each of the Services. Such growth makes more difficult achieving the JTA's goal of facilitating C4ISR system interoperability.

The present DoD communication systems and the functional platforms they support are many and very diverse. The underlying SA framework for these systems is a circuit-centric, system-specific approach that results in an extremely inflexible infrastructure. Communication between platforms requires, in many cases, that another radio be placed on one or several platforms, bandwidth is preallocated and underutilized, and radio spectrum is suboptimally used because of pre-allocation to support multiple networks in the same, or *possibly* the same, geospatial location. DoD modeling and simulation results, several field-training exercises, and numerous studies show that an internetworked, rather than circuit-centric, framework for DoD telecommunications can substantially enhance combat effectiveness—it can make the difference between success and failure.

Although the effectiveness of a DoD intranetwork has been demonstrated, an issue often raised regarding its implementation is its security. The Task Force believes that deploying a secure DoD-wide virtual Intranet is not a technology issue—it is a management and policy problem. Commercial and DoD security technologies are adequate to significantly improve the security of such a DoD infrastructure. However, an overall security architecture and strategy for securing DoD C4ISR (strategic and tactical) systems must be developed. Today, three separate transport networks exist and the Services are pursuing specific individual solutions for their tactical communication infrastructure. Generally, security is an afterthought or a presumed capability.

The management and policy aspect of the security problem can best be illustrated by what is not done or does not exist today. First, surveillance by the National Security Agency (NSA) during the Kosovo air campaign documented several information compromises where security options were available but were not used. Second, no specific actions have been taken in DoD secured intranets (e.g., the Secure Internet Protocol Router Network [SIPRNET]) to mitigate the insider problem; once inside the network, a user has unlimited access. Technology is available to "raise the bar"; as noted earlier, the private sector is reducing the threat from an insider by segmenting and limiting access to corporate databases using Public Key Infrastructure (PKI) in their intranets in combination with intrusion detection systems. Third, the DoD is operating on a no-failure rather than a risk-management security philosophy. While "no failure" is an appropriate policy for exceptionally sensitive information, the rigor and expense associated with

it make it impractical for deployment throughout the DoD infrastructure. Rather, a risk management approach should be invoked as the basic underlying security philosophy. Without a risk management approach, the DoD will have difficulty achieving its operational concept goals such as unattended sensors internetworked among themselves and, through a common-user secure Intranet to the users of the information they collect. Fourth, continuous security awareness and training programs for DoD employees are virtually nonexistent. Fifth, there is no formal and ongoing Red Team (Information Operations) process that tests and evaluates the security of our systems on a continuous basis. Coalition warfare will further exacerbate security management and policy issues.

While much must and should be done to implement a secure DoD-wide virtual Intranet (a GIG), many Service- or system-centric initiatives are underway to provide more communication resources to our warfighters. The Services and OSD are attempting to address communication shortfalls through initiatives such as IT-21, the Tactical Internet, Extended Littoral Battlespace Advanced Concept Technology Demonstration (ELB ACTD), Theater Deployable Communications, Global Grid, the Warfighter Information Network—Tactical (WIN-T), the Joint Tactical Radio System (JTRS), Standardized Tactical Entry Point (STEP)/Teleports, and the joint Military Satellite Communication (MilSatCom) Architecture. All are, independently, addressing communication and networking needs from each sponsoring organization's perspective. Several are attempting to meet military needs while exploiting commercial technology, concepts and infrastructure. Similarly, there is a reasonable DoD Science and Technology (S&T) program to address commercial IT shortfalls through initiatives such as Global Mobile Information Systems (GloMo), Small Unit Operations (SUO), Radio Access Points (RAP), the IA program, Wolfpack, and Airborne Communications Node (ACN).

In many of these initiatives, DoD is making modest progress toward changing its acquisition methods for IT. The progress is best illustrated by C2 for the Next Subsurface Nuclear (NSSN) platform—a JTA success story; IT-21; the Tactical Internet (spiral development); the use of Indefinite Delivery/Indefinite Quantity (ID/IQ) contracts for the acquisition of telecommunications services from the private sector, and the Electronic Systems Command (ESC) study on the spiral acquisition processes. However, in general, DoD still applies the 5000-series acquisition regulations for the acquisition of C4ISR systems, thus accepting a fifteen to twenty-year acquisition cycle; assumes system lifetimes of decades; and does not recognize ownership costs and acquisition costs as total system investment. DoD clearly has not internalized the implications of the rapid turnover rate of IT in the private sector and consequently cannot yet effectively leverage this technology revolution.

Nowhere is the absence of a specific vision and acquisition policy more detrimental than in two current major DoD communications programs—the JTRS and MilSatCom. The former represents a unique opportunity that could be a turning point in military wireless communication infrastructure. The potential impact of the system is clearly under appreciated. It could be the foundation for a common-user, QoS, Internet and could integrate legacy systems into a common-user framework as is occurring in the private sector. Unfortunately, the networking aspects of the system are being lost; the focus of the program remains on duplicating legacy waveforms; minimal network services are being procured, and too few prototypes are being developed to

permit network-service evaluation. The consensus-based acquisition process used for JTRS is driving the program to focus on the past.

Other than for *protected* services, MilSatCom is business as usual at a time when a window is opening for the procurement of new technology and services from the private sector. While the Task Force recognizes the need for some protected military-unique Satellite Communications (SatCom) capacity, much of the military communications needs can be met more cost effectively by using the many redundant commercial systems emerging in the marketplace. Unfortunately, the MilSatCom procurement strategy is directed towards the reprocurement of several military-unique systems with modest enhancements to its twenty-year-old systems. This activity will consume $10 Billion of procurement funds over the next ten years, and nearly an equal amount of operations and maintenance (O&M) funds as well. Again, this is an approach founded on doing business as DoD has done in the past.

Despite the paucity of quantitative requirements specification by the Services and DoD, several significant observations can be made. First, more bandwidth is required to meet today's military communications needs from both a Service and a joint perspective. Second, interoperability issues must be resolved even within a Service's C2 systems and communications infrastructure. Third, the CINCs have the same interoperability problems and communication needs as the Services, but compounded by having to integrate the Services' communication infrastructure as well as those of coalition partners. Finally, all DoD communication acquisitions currently anticipated over the next ten years will not, in aggregate, meet the anticipated requirements.

In summary, real-world experience and analysis show that exploiting commercial communication/security architectures, technologies and systems are critical if we are to adequately support our warfighters. The Task Force findings clearly show that the DoD communication-infrastructure vision; acquisition strategy and resource planning will not meet war-fighter needs now or in the future. To mitigate this situation, the goal should be to minimize the use of DoD-unique systems and focus their use only on a minimal, essential, highly-protected backup network and exploit the vision, technologies and systems being developed in the private sector. There is a very complex set of trade-offs that must be analyzed to establish the appropriate mix of commercial and DoD-unique telecommunication systems. DoD is not currently structured, nor does it have independent resources, to conduct such an analysis. Based on these findings, the Task Force offers the following recommendations

RECOMMENDATIONS

Recommendation I—Information Superiority Board

The Task Force recommends that the Secretary of Defense (SecDef) establish a DoD "Information Superiority" Board of Directors (BoD) to provide oversight and governance for the realization of DoD-wide GIG. Membership on the BoD should include: Deputy Secretary of Defense (Chair), USD/AT&L, ASD/C3I and the Vice Chairman–Joint Chiefs of Staff. This board should be impaneled immediately.

In order to provide high-level, knowledgeable, independent advice regarding commercial technologies, applications, and trends to this BoD, the Task Force recommends that the BoD

establish an Advisory Group that draws on senior, private-sector individuals (with prior DoD experience) who are leaders in the areas of Internet technologies, commercial security technologies, emerging commercial satellite systems, and the like. This group should be impaneled by 31 January 2000.

Recommendation II—DoD Vision for GIG

The Task Force recommends the establishment of a DOD vision, policy, and requirements for an integrated, common-user, QoS-based, DoD-wide virtual Intranet.* The first release of documents should be by 31 May 2000 with updates following semi-annually to reflect evolving commercial Internet technologies.

Recommendation III—Standards-Based GIG

The Task Force recommends the development of policy and requirements for a commercial-standards-based, common-user, QoS-based, DoD-wide virtual Intranet using IP as the convergence layer. The Panel also recommends ASD/C3I implement a process to reduce JTA standards and protocols to a minimum essential set that, at its core, should be predominately commercial.

The Task Force recommends that ASD/C3I and USD/AT&L establish a policy and review process that requires all DoD information and communication systems to adhere to commercial IP naming and addressing conventions, and that the JCS establish the requirement that all DoD communication systems be able to interpret and route IP datagrams. Recommendation III should be accomplished by 31 March 2000.

Recommendation IV—GIG Implementation Process

The Task Force recommends that the Information Superiority Board of Directors establish an Executive Office responsible for leading and implementing the DoD-wide, common-user virtual Intranet, the GIG. We recommend that the office and leadership position be established by 29 February 2000.

It is recommended that the Executive Director be a minimum five year appointment and be tasked to develop an implementation plan, including technical milestones and measurable interim goals, and identify resources to permit the transition to and completion of the GIG by 30 September 2003. It is further recommended that system-engineering support be provided to the Executive Office through a dedicated system engineering team. The Task Force recommends that the Implementation Plan for moving from DoD's present circuit-based infrastructure to the GIG be developed by 31 October 2000 and updated semi-annually.

It is recommended that the Executive Director, with support from ASD/C3I and USD/AT&L, task all DoD and Service Program Managers/Program Executive Officers (PM/PEO) responsible for tactical/strategic telecommunication systems to conduct studies on how to transition their system to permit integration into a common-user DoD virtual Intranet. Furthermore, the Executive Director should fund two competitive industry studies that address

---

*A virtual Intranet is a virtual private network, secured by cryptographic means that operates, with service guarantees, over the commercial Internet.

how (not if) emerging commercial communication satellite systems, fiber infrastructures and mobile Internet technologies can be exploited to implement the DoD-wide virtual Intranet. These studies should be completed by 31 July 2000.

Based on this study's results, it is recommended that the Executive Director be given the task to transform DoD communications from a circuit/broadcast and system-centric framework to a common-user, internetwork framework.

Recommendation V—Information Security

The Task Force recommends that OSD and the Service Chief Information Officers (CIOs) should, under OSD leadership: set security policies and procedures; leverage commercial practices, technologies and investment; and formulate/execute a "balanced mix" security architecture and strategy for the GIG. It is recommended that the policy, procedures, and strategy be in place by 30 August 2000 and that the Executive Director be tasked to implement the architecture and strategy.

Recommendation VI—Empower the Customer

The Task Force recommends that the SecDef provide acquisition authority and resources to a CINC representative with a charter to buy off-the-shelf commercial telecommunication services to augment service-provided infrastructure, as required, to meet joint warfighting needs. Specifically, it is recommended that the charter of the U.S. Space Command be expanded to include information and telecommunication systems—a CINC IS. It is further recommended that the CINC IS acquisition authority for nondevelopmental commercial IT services be resourced by the allocation of a modest 10% of DoD's C3 yearly funding. The resulting level of resources would be about $1B per year. Also, the Panel recommends that Joint Forces Command (JFCOM) be resourced to be the experimentation and evaluation agent for the GIG that would evolve as Recommendations I through VI are implemented.

Recommendation VII—DoD S&T for GIG

The Task Force recommends that DoD Science and Technology (S&T) initiatives be focused to augment commercial technology only where absolutely necessary. It is recommended that the Director, Defense Research and Engineering (DDR&E) and Defense Advanced Research Projects Agency (DARPA) address extensions to commercial standards/protocols/technology to meet specific DoD needs. Further, it is recommended that DDR&E, through the Service Laboratories, undertake the mission to have DoD needs presented and supported in commercial-technology standards forums.

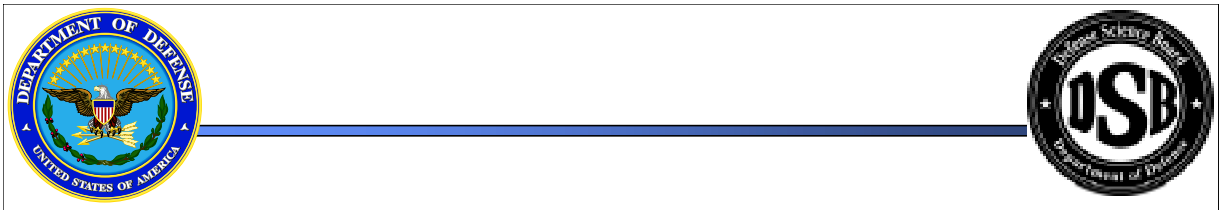
Recommendation VIII—JTRS Program Recovery

The Task Force recommends that its January 1999 JTRS report and recommendations be implemented by 31 March 2000. The JTRS program must be redirected to meet the Operational Requirements Document (ORD) networking requirements. The USD/AT&L, ASD/C3I, and J6 must ensure that JTRS realize its potential and requirement to be the foundation system for realizing a DoD common-user, adaptive, flexible, QoS-based communication infrastructure.

CONCLUSIONS

The DoD must exploit the private sector's Internet telecommunications technology, architecture, standards, and systems as a strategic means to meet our warfighters' information and decision superiority needs. Providing adequate telecommunications resources to our warfighters is an imperative—a must-do as important as providing weapons, sensors, food and the like. DoD's present vision, understanding of requirements, and acquisition strategy for present and future communications infrastructure are inadequate to meet our warfighters' needs. A strategic mix of mostly private sector telecommunication technologies and systems (leased or bought) combined with a smaller subset of DoD-unique systems integrated into a common-user DoD-wide virtual Intranet must be the goal for the future.

Today, this "mix" happens on a crisis-by-crisis basis: Kosovo could and would not have been successful if we had not procured, in real time, extensive private sector telecommunication services for DoD use in this contingency. It was a difficult, high-risk, save-the-day approach to meeting the C4ISR information transport needs for this contingency, but it worked! We can and must make the Kosovo exploitation of private sector telecommunication systems and technology the cornerstone of our approach for the future. Let us not leave to crisis implementation what should be a strategic plan for DoD. Building the DoD GIG on this strategy must proceed immediately.



Defense Science Board

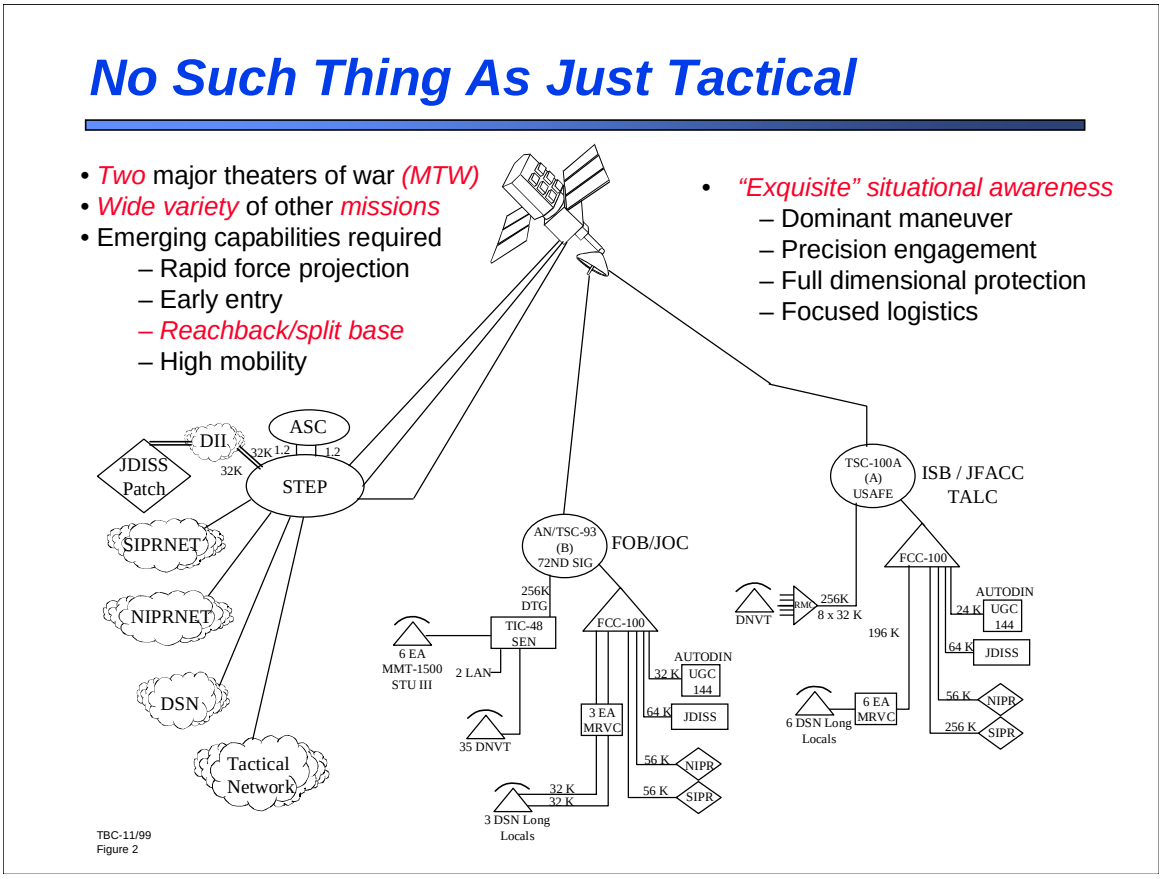
Task Force on

TACTICAL BATTLEFIELD COMMUNICATIONS

Final Report
November 1999

TBC-11/99
Figure 1

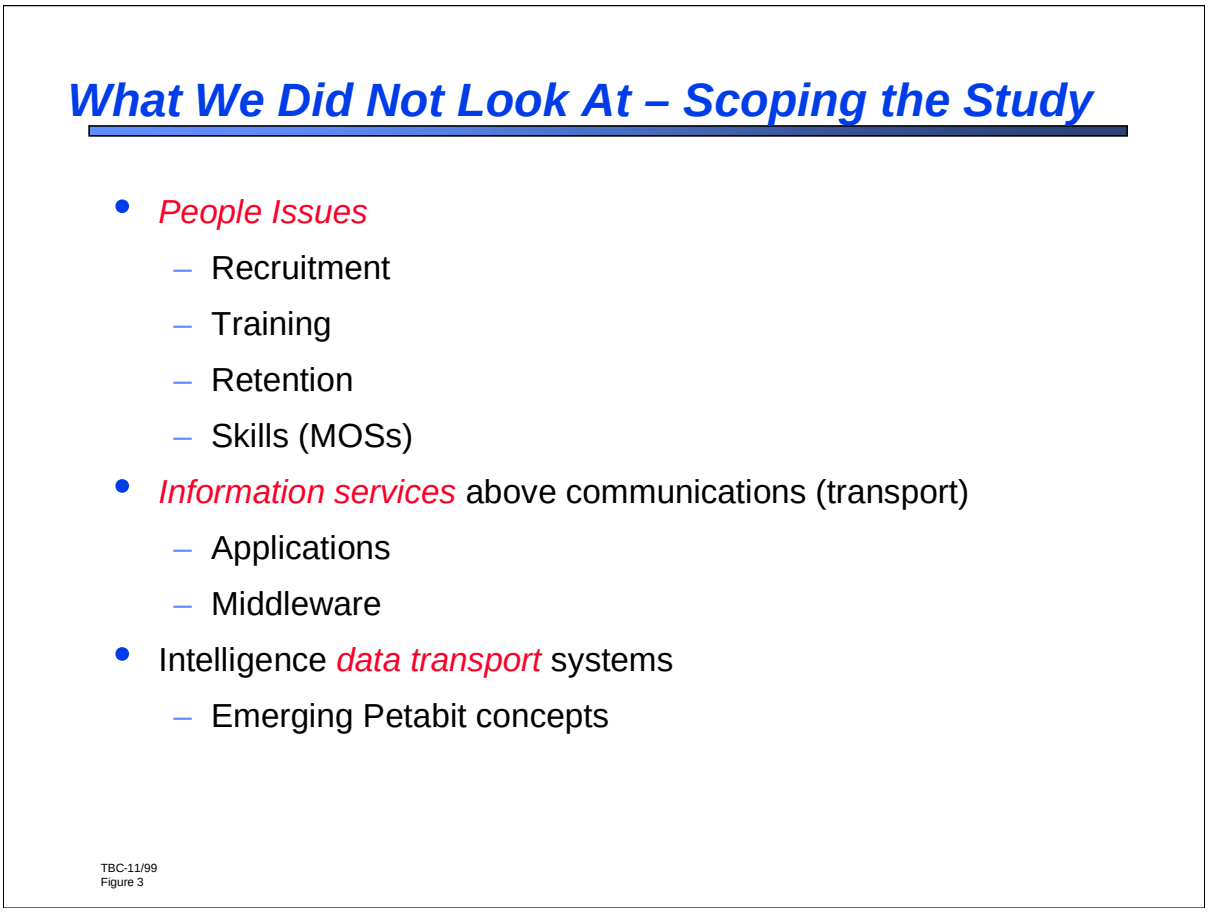
1 INTRODUCTION



In the fall of 1998, the Defense Science Board* was asked to conduct a study on Department of Defense Tactical Battlefield Communications. The Terms of Reference (TOR) for the study were finalized in the last quarter of calendar year 1998, and Task Force members were selected in preparation for a kickoff meeting in November of that year. As a result of discussions with sponsor representatives and as a result of briefings obtained at the Task Force's first meeting, it became clear that "Tactical Communications" could and should not be restricted only to "in-the-field" systems. As noted in Figure 2, emerging warfighting concepts predicated on force-projection, split-base operations, early entry, reachback and the like implied that tactical communications must include the integration of post-camp-station communications and other DoD strategic and operational communications resources with systems deployed to the field. This observation was reinforced by the Service briefings and Intelligence community briefings as well as by briefings from the Commanders-In-Chief (CINCs) received by the Task Force. In fact, in the CINCs' briefings, the argument was made that access to information services on DoD's Secure Internet Protocol Router Network (SIPRNET) and its nonsecure counterpart (NIPRNET) was required in the field in the same manner that these services are available to the desktop in

*An acronym list is provided in Annex E of this report.

post camp and station. As a result of these findings, the Task Force decided that the distinction between tactical communications and strategic, or post camp and station information infrastructure was not useful or realistic. Our warfighters expressed the need for a ubiquitous, fully integrated communications infrastructure that provides information transport services among all sources and users of information worldwide—their bottom line was there is "no such thing as just tactical" communications.



Therefore, at its first meeting, the Task Force increased the breadth of its study to include not just the in-the-field communications infrastructure, but all communications required to support our warfighters in whatever contingency operation they had to support. Given this expansion in charter, and in order to keep the scope of the study tractable, the Task Force set boundaries for the study in three areas as indicated in Figure 3.

First, the Task Force decided that it would not address issues associated with the recruitment, retention, and training of personnel. The panel realized that the Services would experience increasing pressure from the private sector for personnel with Military Operations Specialties (MOS) or expertise in the area of communications. The rapid introduction of

Information Technology (IT*) in the private sector has created a demand for people with technical training in this field. This demand causes difficulties in recruiting and retaining individuals with these skills in our Services.

Furthermore, as DoD continues to exploit commercial IT, the training of military specialists in areas such as digital communications, Internet** management, Internet system architecturing, and Internet protocols and standards will be a growing requirement. As our military personnel acquire these skills, they will be aggressively sought after in the private sector. This issue needs further attention within DoD, but was not addressed in this study.

Similarly, the Task Force limited its attention to the communications transport component of what should eventually be a DoD-wide virtual Intranet or Global Information Grid (GIG) (also named the Integrated Information Infrastructure—see DSB Summer Studies for 1996 through 1999). In the layered reference model for the private-sector Internet, the transport layer is the component that moves digital bits from any source(s) of data or information to user(s) requiring or requesting them. The transport layer provides telecommunications services to the layers above (middleware and applications). In the context of DoD, the middleware and applications layers are typically integrated into Command and Control (C2) and Intelligence, Surveillance, and Reconnaissance (ISR) systems. The Task Force chose not to address, in any detail, issues associated with the design, acquisition and fielding of DoD's C2ISR infrastructure.

Finally, the Task Force did not consider emerging concepts or systems for intelligence-data transport. The movement of raw data from the sensors to centralized processing sites in the continental U.S. (CONUS), or other such sites, will require very high-capacity communication systems. Given the capacities being considered, the Task Force noted that the total anticipated C4ISR traffic for two Major Theaters of War (MTW) would be less than 3% of the total predicted intelligence data. The question arises as to whether the intelligence data transport system could be architected to support all of DoD broadband data transport needs. This question was not pursued by the Task Force.

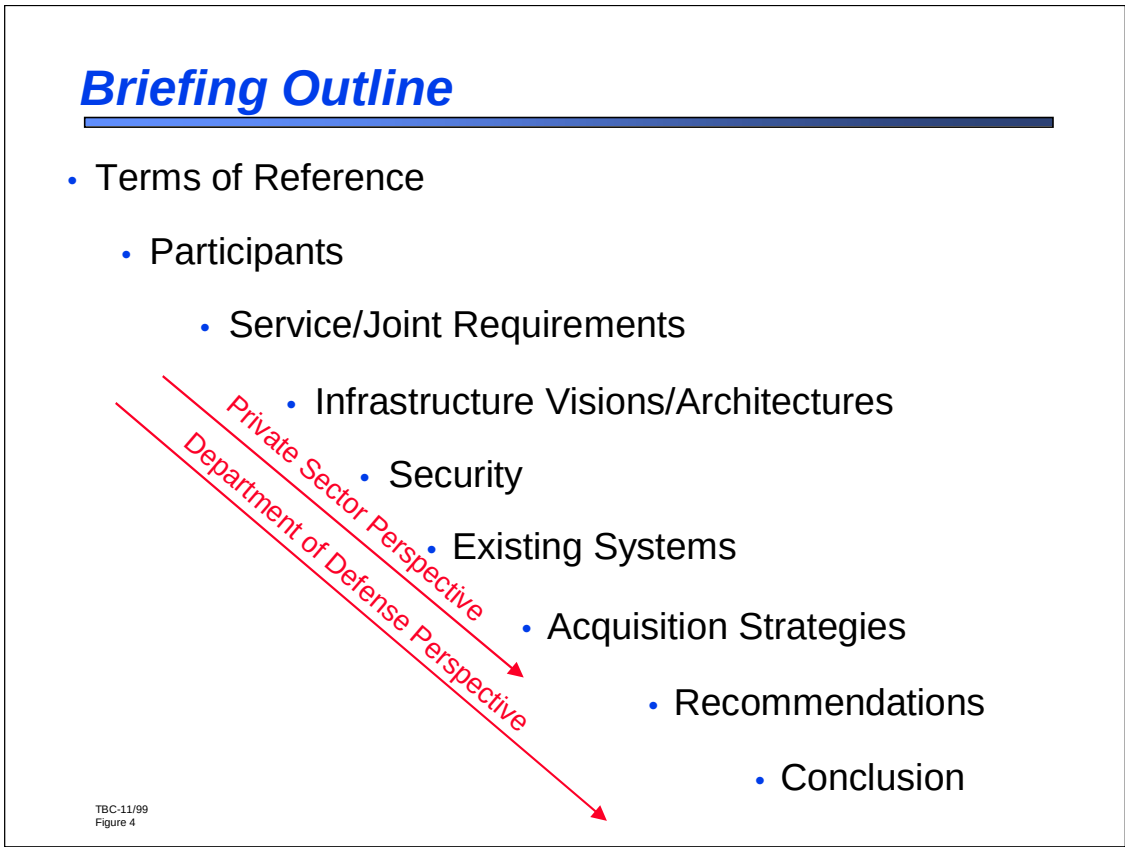
The study did, however, consider the requirement of transporting intelligence product and data from theater sensors to processing and senior command facilities wherever they are situated, as well as the dissemination of intelligence products from these facilities to theaters of operation.

Once the Task Force scoped its study, it established major topics for the briefings it wished to receive over the following twelve months. The topics were selected to ensure a sequence of briefings that would cover the TOR in a logical manner; each set of briefings building on the ones the Task Force would have received in preceding meeting.

---

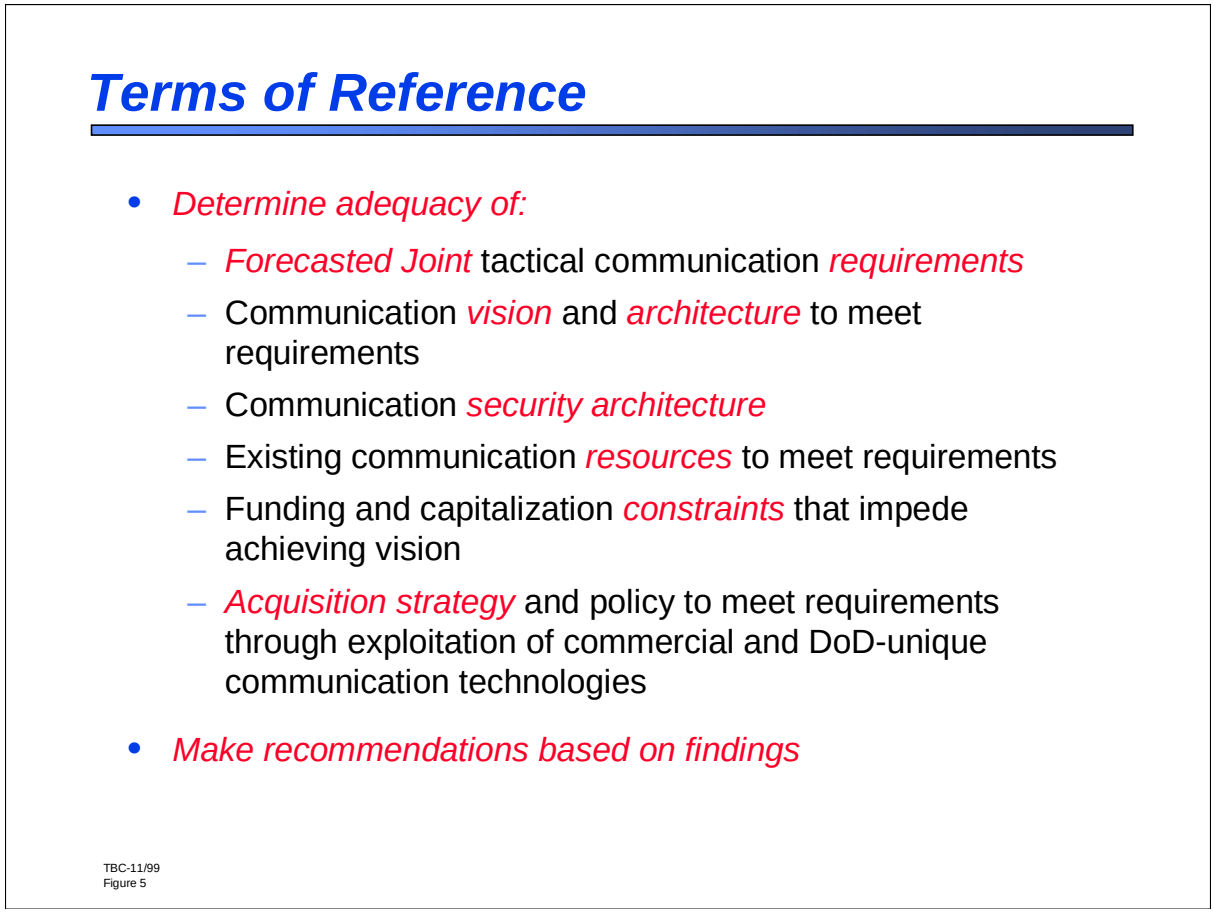
*In this study we include communication/telecommunications technology under the general term of Information Technology.

**Internet technologies are those related to, or incorporated into, the commercial Internet—sometimes referred to as the World Wide Web.

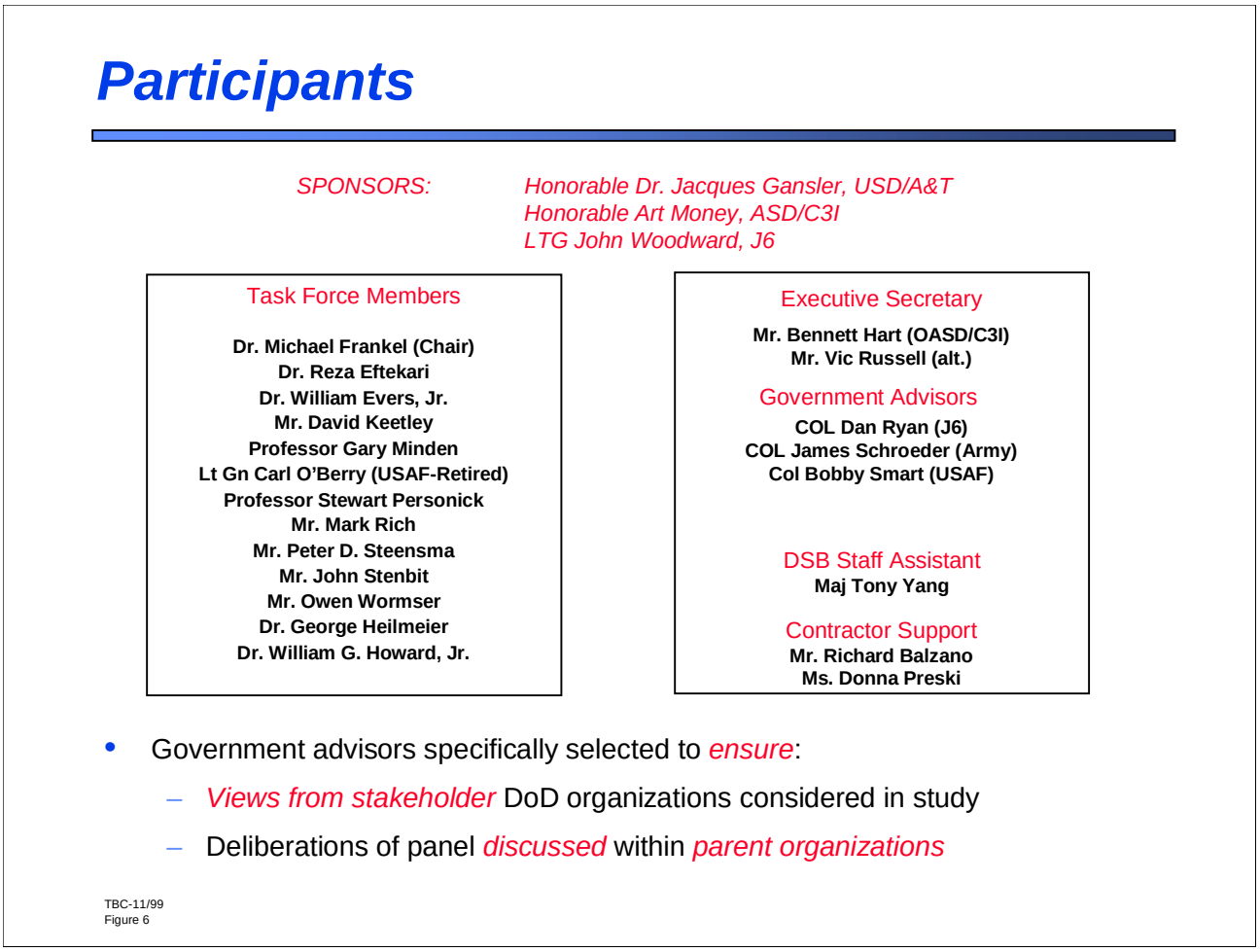


The Task Force also decided to address the TOR from two perspectives, as noted in Figure 4—from a DoD standpoint, as requested by the study's sponsors, and from a parallel private-sector perspective. This two-step process through the TOR was felt to be critical, given the rapid development and introduction of transport infrastructure and technologies into the consumer marketplace and because of the emerging DoD goal of trying to exploit commercial IT where and when appropriate. This study structure, which forms the basis of this report, provided the Task Force the information necessary to more fully address its charge from the study sponsors.

Consequently, this report is structured as indicated in Figure 4. It first addresses findings from a private sector perspective on commercial telecommunication requirements, the vision and architectures that exist in the private sector for the evolution of commercial telecommunication infrastructure, the existing technologies that are used, and the acquisition strategies used to acquire and deploy new technologies. The report then addresses these same issues from a DoD perspective. The study compares the two sector approaches for implementing telecommunications infrastructures, it makes comparative observations, and then presents recommendations.



Thus, the structure of the report and the manner in which the Task Force proceeded to acquire information was in direct support of and guided by the TOR set for the study. For each item of the TOR, synopsized in Figure 5 and provided in its entirety in Annex A, the panel took in-depth briefings from numerous DoD and private-sector organizations. Task Force discussions about the briefings and resulting findings related to the material presented were captured in meeting minutes and the briefings themselves were compiled into on-line and hard-copy libraries for Task Force use during its deliberations and recommendation formulation.



The DoD sponsors for the study, and ultimately the individuals who established and approved the TOR were: The Honorable Dr. Jacques Gansler, USD/AT&L, the Honorable Art Money, ASD/C3I and LTG John Woodward, JCS-J6.

The Task Force membership (Figure 6) included communications/networking experts from government, private sector and academic organizations. As the biographical sketches in Annex B indicate, these individuals collectively have extensive experience in telecommunications (digital and analog) technology invention, development, and deployment. Member experience also included senior positions within DoD with responsibility for delivering telecommunication and other systems and services to the warfighter, experience in computer networking from senior academic as well as DoD Science and Technology positions; and senior leadership experience in consumer and DoD telecommunication systems and technology. The individuals with this breadth and depth of expertise were carefully selected to ensure that all aspects of the TOR could be adequately addressed.

The Task Force executive secretaries were Mr. Bennett Hart and Mr. Vic Russell, both from the office of the ASD/C3I. They helped identify briefings the Task Force should hear and they provided feedback to and from one of the study's sponsors. Government advisors included

representatives from the Services and J6. Several of these individuals took an active role in helping the Task Force gain access to important briefings; they helped bring to the study ideas and issues from their respective organizations; and they carried to their organization the findings and preliminary recommendations of the panel to their organizations for comment.

Finally, the team was supported by two individuals provided under contract to the DSB. These individuals were responsible for agenda setting, meeting logistics and general administrative support to the Task Force. Their assistance was critical to the efficient and effective conduct of the study, for which assistance the Task Force is immensely grateful.

Meeting Schedule/Planned Topics

1998	Briefings Received	Subject
Nov 19-20	11	Kick-off and special review of *Joint Tactical Radio System*
1999		
Jan 11-12	14	Adequacy of DoD communication vision and architectures capable of meeting forecasted service and joint requirements
Feb 18-19	12	Adequacy of companion communication security architecture to assure protection and information assurance
Mar 18-19	6	Funding and capitalization constraints that restrict ability to make the transition from equipment in the current inventory to equipment needed to meet the evolving communications requirements
Apr 22-23	5	Adequacy of tactical communications equipment now in the DoD inventory, or under development, to fulfill the evolving communications requirements, to include, operational experience with communications equipment in ATDs and ACTDs
May 20-21	9	Panel discussions
June 24-25	6	Adequacy of acquisition strategy and policy to meet communication architectures and requirements that facilitates exploiting of commercial and DoD-developed technologies and services
Jul 22-23	7	*JTRS Program update,* Security briefings and Panel discussions
Aug 5-6	0	Panel discussions
September 9-10	4	Acquisition briefings and Panel discussions
October 7-8	0	Panel discussions
November 18-19	0	Finalize report

TBC-11/99
Figure 7

The meeting schedule the Task Force set for itself is shown in Figure 7. As noted earlier, for each two-day meeting a specific topic in the TOR was addressed. For each topic, the team members identified a series of briefings they wished to hear and the Executive Secretary and support team scheduled the speakers. During each meeting, Task Force discussion was also scheduled in order to permit debate and ultimately consensus to be reached on findings and recommendations. The agendas for each meeting provided in Annex C, brought individuals from many DoD and private sector organizations to the Task Force. In total, over 70 briefings, from a similar number of organizational entities, were received. It was this material, the Task Force

members' background and expertise, and the many discussions that ensured that lead to the findings and recommendations that follow.

As noted in Figure 7, one topic—the JTRS was addressed at the first meeting. This out-of-sequence topic was assessed early in the study at the request of the sponsors. The Task Force members reviewed the JTRS program—its vision, mission, and technology development strategy, and reported its findings and recommendations within a 30-day window. This report is provided in Annex D in its entirety; and an update review on the program, conducted in July 1999, is presented in the main body of this report.


Private Sector Findings
TBC-11/99
Figure 8

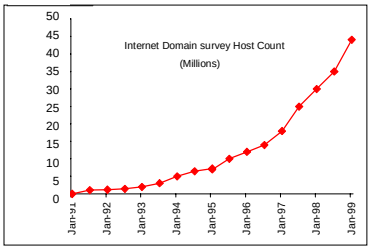
Findings: Private Sector – Requirements

- **Internet Subscribers 1999**

World Total	171.25 Million
Africa	1.14 million
Asia/Pacific	26.97 million
Europe	40.09 million
Middle East	0.88 million
Canada & USA	97.03 million
Latin America	5.29 million

Compiled by Nua Internet Surveys

- **Internet Host Sites**



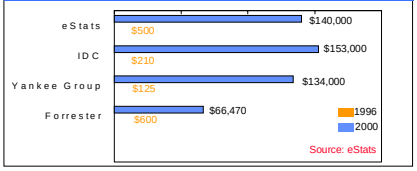
- **Internet Revenues - The Engine**

Comparison of Online Revenue Projections (Millions)

Year	EStats	Forrester	Multi-Media Research Group	Jupiter	Cowles/ Simba	IDC
1995	$450	NA	$350	NA	$614	$1,000
1996	$750	$518	$520	$575	$993	NA
1997	$1,500	$1,138	$850	$1,250	NA	NA
1998	$3,700	$2,371	NA	NA	NA	NA
1999	$6,100	$3,990	NA	NA	NA	NA
2000	$10,000	$6,579	$6,500	$7,300	$4,270	

Source: eStats

Business-to-Business e-commerce Projections (Millions)



e-commerce will be a trillion dollar industry by 2003

Source: Forrester

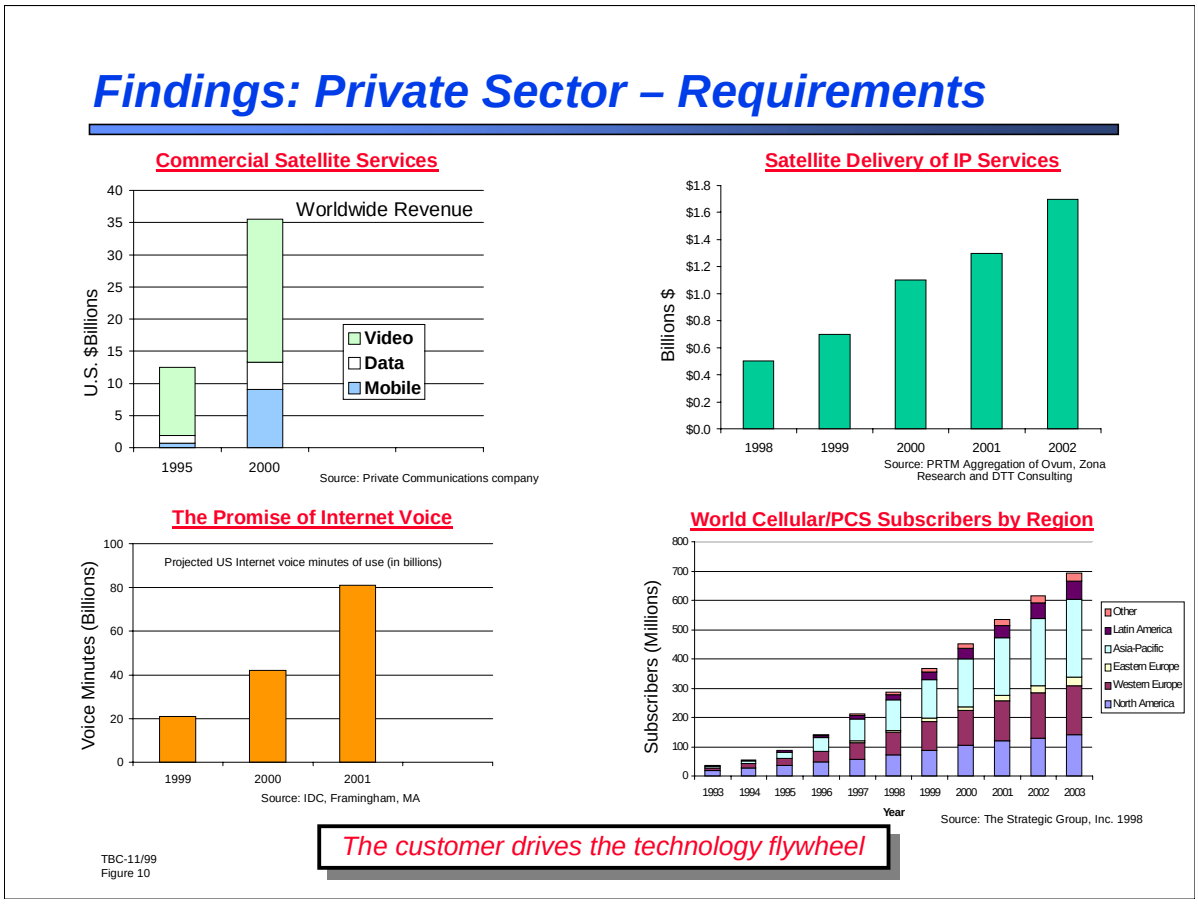
TBC-11/99
Figure 9

In addressing the TOR from a private sector perspective, the Task Force noted that (tele)communication and IS technologies development and deployment are being focused primarily on augmenting the capabilities, or extending the reach, of the Internet (World Wide Web [Web]). In an attempt to understand what requirements for the Internet the telecommunication industry is trying to satisfy, it became clear to the Task Force that private-sector customers do not, in general, express their requirements for Internet services in terms of bits per second (bps) or types of information to which they desire access. Their requirements are typically expressed in qualitative terms such as faster response, continuous availability, reliable access and services, and the like. The telecommunications industry is therefore responding more to anticipated needs than to quantified requirements.

This industry response is stimulated by the success of the Internet over the past decade. For example, the number of Web sites on the Internet has grown exponentially, year by year, worldwide. As indicated in Figure 9, in 1999 there were an estimated 171 million Internet users and over 40 million host computers. More importantly than the number of users and hosts, the Internet (World Wide Web) has changed the way many people access news, students research papers, and people purchase goods and services. Its influence and capabilities are challenging the way many business sectors operate: music publication and distribution, and the delivery of Internet newspapers, radio, and television, are but a few examples. In 1999 commerce over the Internet amounted to approximately $5 billion. By 2003, it is expected that over $1 trillion of commerce will take place over the Internet.

This phenomenal growth in the Internet and its impact on the conduct of business worldwide comes about in part from the information and services provided therein, but more

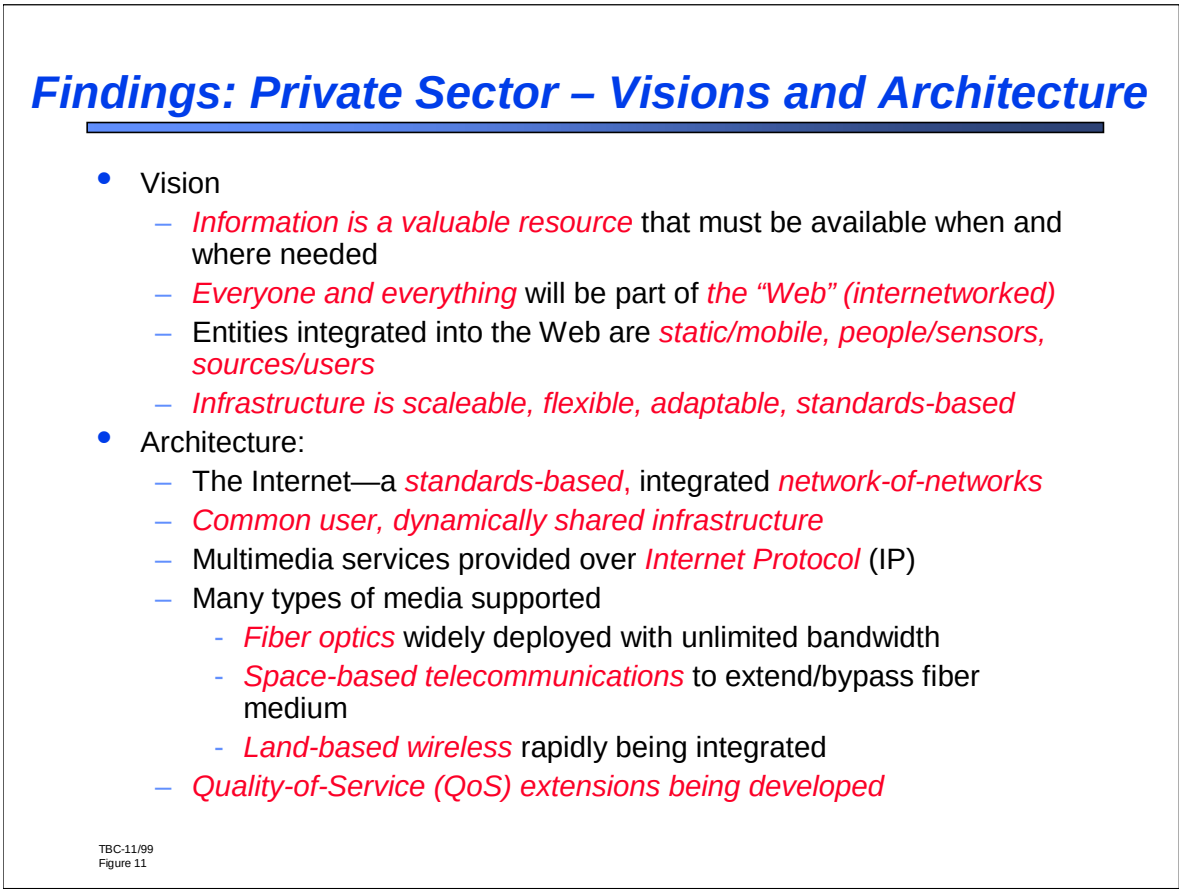
importantly from the ubiquitous access to and flexibility of dynamically shared information among users. The fact that information can flow between any set of users at any time has enabled dynamic business relationships and processes to develop in unanticipated ways. On-line, real-time financial transactions (consumer to business and business to business) occur as needed, when needed. On-line auctions of goods and services have materialized in less than a year; on-line multiparty game playing has become a growing industry; and many other multiparty virtual communities supported by many varied information services have come into being virtually overnight. In fact, it is argued that the value of the Internet is that it permits individuals and organizations singly or in communities of interest to exchange information when and as needed. Pundits argue that the value of the Internet increases as the square of the number of subscribers it supports.



The value of the Internet as an information appliance is evidenced by the growing number of services it supports. In addition to text-based information caching, storage and dissemination services, similar services are beginning to emerge for video and imagery. Furthermore, a new service, Internet telephony or Voice over Internet Protocol is rapidly emerging.

In addition, new telecommunication systems are being deployed to meet consumer demand. In all cases, these services are stimulated by anticipated revenue generation as shown in Figure 10. The services include the cellular and personal communications (PCS) services being deployed worldwide; commercial satellite systems to provide voice, and narrowband data services are also proliferating.

Another area of infrastructure growth is the integration of broadband satellite telecommunication systems into the Internet. Although the use of satellite channels as trunking facilities within the Internet have been in use for almost two decades, several of the next-generation satellite systems will provide packet-switching services and serve as a network integrated into the Internet—the network of networks. Although terrestrial PCS, today's space-based telecommunication systems, and the Internet have evolved independently, market forces are motivating their convergence. Within the next few years, all such telecommunication systems will become an element within the private-sector integrated information infrastructure.



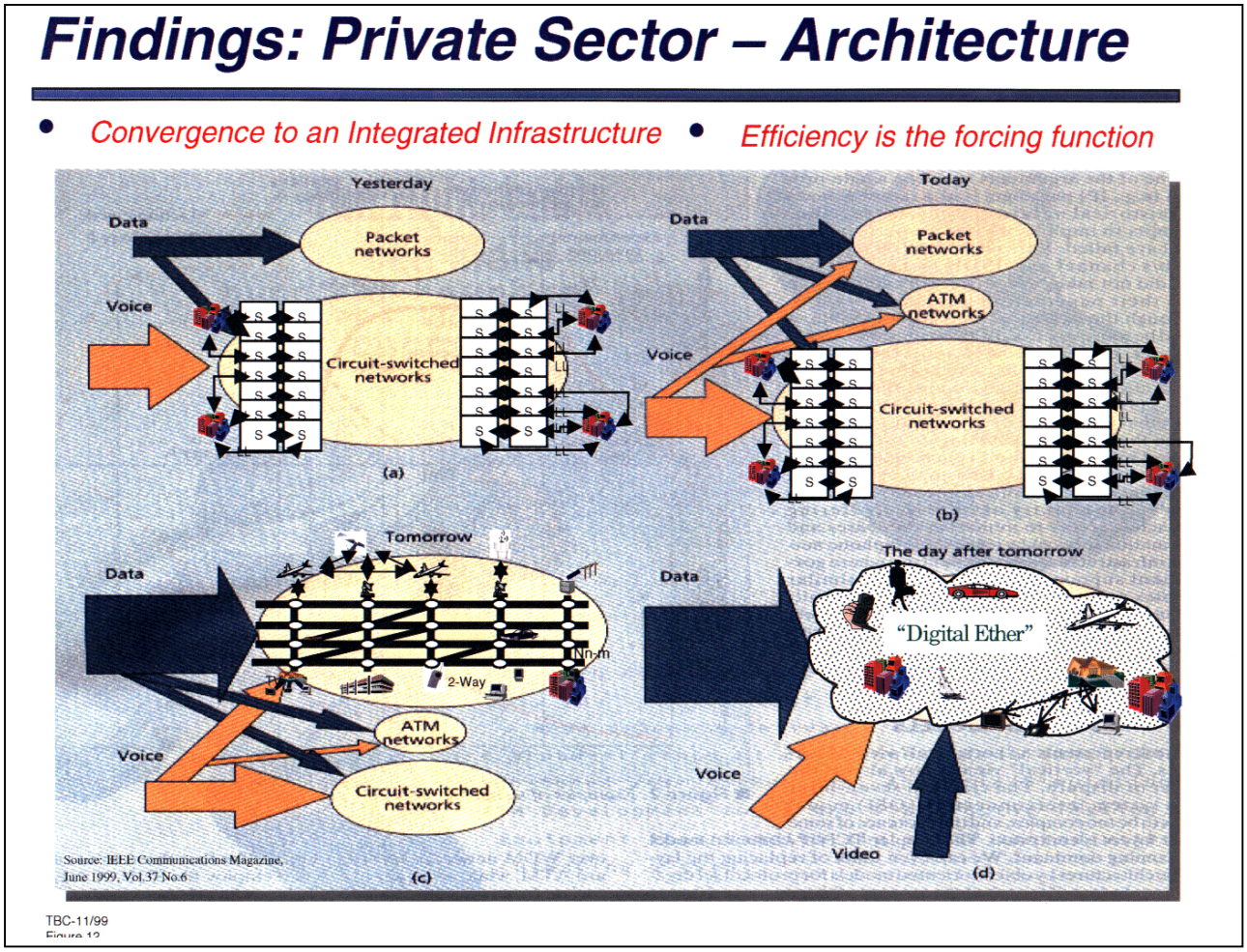
What is driving this convergence is the realization in the private sector that information is a valuable and critical resource for the conduct of efficient business. Businesses have used information—accounting records, personal records, inventory, and the like—since the invention of writing. Only during the past ten to fifteen years has the value of timely information, information at the right place and at the right time, been recognized, and only in the past five years has the value of interlinking information resources been exploited. The private sector is progressing toward a vision that all information resources will be integrated into a "Web." This integration will change how individuals buy commodities (e-commerce); how commodities are delivered (consumables, newspapers, radio, TV, and music); and how business-to-business transactions are carried out.

The evolving web of interlinked information resources is based on an architecture that is scalable, flexible, and adaptable. The architecture is scalable in the sense that the same mechanisms that help to build a small-business local web also can support a multinational corporation. The architecture is flexible in that the Web operates a heterogeneous collection of communications, computer, and application systems. And, the architecture is adaptable such that as new technologies are created they are easy to integrate into the expanding Web.

The Web or Internet expresses these attributes of scalability, flexibility, and adaptability for two reasons. First, the Internet is based on a small and relatively simple set of open standards

and protocols. "Simple" means that the protocols are easy to implement and adopt and "Open" means anyone can use the protocols because they have well-defined application program interface (API) specifications, are ubiquitous, and are supported by numerous private-sector companies. Second, from its inception, the Internet was designed to be a network of networks, hence the name. Thus, the concept of scalability was inherent in the conception of the Internet. It is relatively easy to add another network, a feature that has resulted in the Web's exponential growth, as indicated earlier. Thus, the architecture framework of the Internet consists of common, ubiquitous, and simple protocols operating over a wide range of the telecommunications medium supporting a rich set of information types and services.

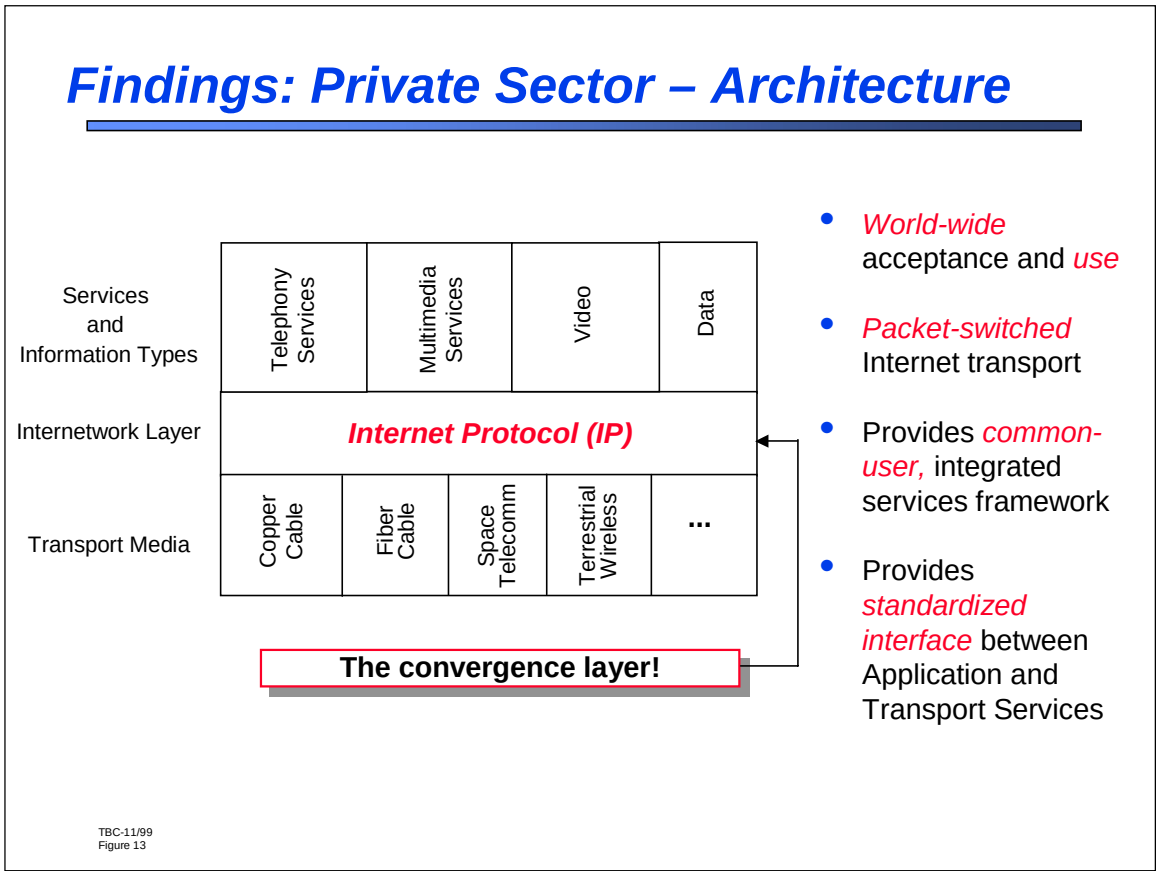
Many kinds of entities are integrated into the Internet. Entities can be static or mobile, they can be people or sensors or actuators, they can be information sources or users. The media over which the Internet operates include fiber optic cables that are widely deployed. Range and coverage is being extended by utilizing satellite based telecommunications systems and mobility of users is increasingly supported with the integration of next generation wireless technologies, such as third generation PCS, and Cellular Digital Packet Data (CDPD) technologies (among many others).



The growth of the Internet in the context of its subscriber population, the multimedia services it supports, and its worldwide ubiquity, are causing a revolution in the telecommunications industry. Over the past few years and at an ever-accelerating pace, a shift is occurring in the private sector from what was a circuit-centric, system-specific architectural framework, built on point-to-point or point-to-multipoint circuits, to a shared, common-user, packet-switched infrastructure. This shift, depicted in Figure 12, is motivated by the realization that the circuit-based architecture is inefficient (bandwidth inefficiently utilized) for bursty data telecommunications—this fundamental issue is a key factor in the emergence of the Internet. What is more important, however, is that the Internet has matured from carrying just computer-to-computer traffic and is now supporting people-to-computer and people-to-people telecommunications. As a result, the shift from a point-to-point to a common-user infrastructure has become much more aggressive. As the Internet provides services to support both real-time and non-real-time applications, the convergence of our national (and international) telecommunications infrastructure to a common-user, packet-switched, dynamically shared network of networks will accelerate.

In the early 1990s a new technology called Asynchronous Transfer Mode (ATM) began to gain popularity. ATM promised to integrate circuit traffic with packet networks to provide a single point of service and to guaranteed QoS. While ATM networks are still present in the backbones of global-scale telecommunications networks, packet-switched networks continue to be widely used in offices, buildings, and global networks. In the year 2000 time frame, projections are that the amount of data traffic will exceed the amount of voice traffic in our nation's telecommunication infrastructure.

New capabilities, most importantly implementing guaranteed QoS, multicast, real-time delivery, and security, are continually being introduced into the Internet. As these capabilities become widely available, voice, video, and data services will be provided on a single, integrated network of networks (typically shown as a cloud in graphics representing the Internet). This visual symbol conveys the underlying architectural framework of the Internet—an infrastructure that lets user(s) share, when, and in the way desired, information with any other user(s).

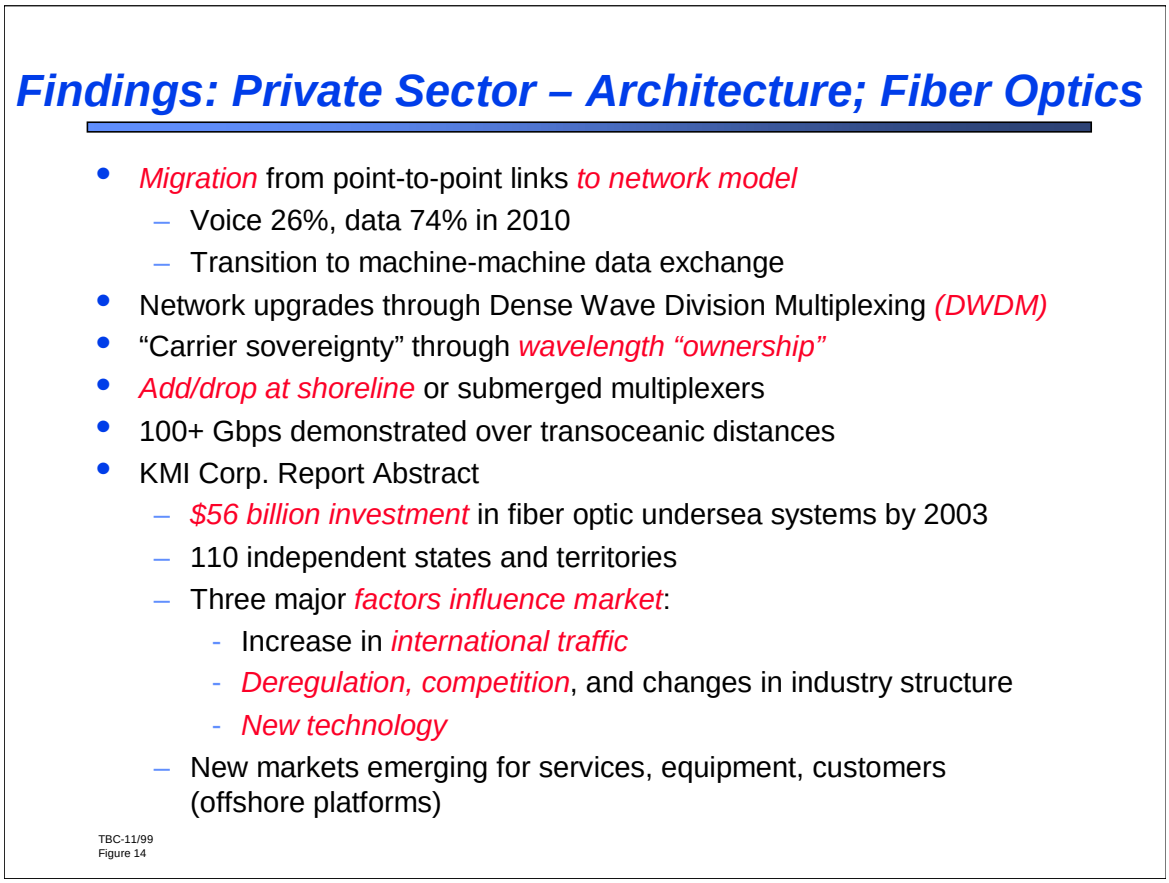


This trend to a common, shared infrastructure for all multimedia services is termed "convergence" in the private sector. The convergence is facilitated by and expected to occur through a common, ubiquitous protocol—IP. This protocol is an open standard supported worldwide by the data telecommunications industry; it is rapidly becoming the convergence layer for all information services on the Internet, as shown in Figure 13.

The common IP layer separates the task of telecommunications (transport) from the tasks of service types, information types, and application development. Network engineers concentrate on moving IP packets from one place to another, independent of their content. Application and service developers concentrate on applications and count on the IP layer to provide requested telecommunications services.

The present version of the IP, designated Internet Protocol Version 4 (IPv4), does not yet support QoS-based dynamic resource allocation, a capability needed to support real-time, stream-oriented information flow (e.g., real-time voice and video). In the near term, this limitation is being addressed through higher-layer protocols such as Real-Time Protocol (RTP), Resource Reservation Protocol (RSVP) and tag switching. In addition, extensions to IPv4, to include a minimum level of QoS, are being investigated by the Internet Engineering Task Force (IETF). The IETF is also working on the next generation of IP, called IPv6, which will include QoS (called differentiated services) and a much larger IP address space, permitting the integration into the Internet of embedded processors (sensors) and many more addressed devices as users.

Today IP is used over many dissimilar networks including: ATM, Ethernet, wireless 802.11, Cellular Digital Packet Data (CDPD) and the like. IP was designed to be the mechanism for transparently moving bits across such networks. Thus, IP is the mechanism that permits the integration of these many types of networks into a network-of-networks; that is, the Internet.



As the demand for services on the Internet grows, the data and voice telecommunication industries are responding by introducing more and varied transport media into the infrastructure. One media, fiber-optic cable, has become the source of the trunks (links) between Internet backbone switches. As noted in Figure 14, one market research firm, predicts that by 2003 investment in submarine fiber optic systems will more than double from today, to a total of $56B. This undersea fiber-optic network will reach 110 independent nation-states and territories. Three major factors are motivating the investment in submarine fiber optic systems: (1) a continuous increase in international data traffic driven by increases in international business, (2) the deregulation and opening of the global telecommunications market, and (3) the development of new fiber-optic technology, enabling significant capacity increase over existing systems at much reduced costs per bit.

Three technologies in particular enable this international capacity and service increase: dense wave division multiplexing (DWDM), optical amplifiers, and add/drop multiplexers. DWDM promises to carry 100 or more individual channels, each either 2.4 or 9.6 Gbps, over a single fiber. Consequently, a single physical fiber can carry almost 1 Tbps instead of the 500 Mbps to 2.4 Gbps of past systems. Separate wavelengths can be sold or licensed to different service providers, who can then provide international network services to end customers. The second technology, optical amplifiers, allows optical signals to be amplified in the optical domain without detection, regeneration, and retransmission, a relatively expensive operation.

Submarine fiber optic systems also include submerged add/drop multiplexers (ADMs). These ADMs allow a few wavelength-defined channels to be stripped from the fiber and routed ashore to a point of presence (POP) and allow traffic from shore to be multiplexed into the data stream on the passing undersea fiber-optic cable. These ADMs may be put into place when the fiber system is installed, but not called in to use until needed.

In addition to supporting broadband trunking (links) between Internet and voice switches, fiber-optic cables are starting to appear in corporate intranets and are providing network access links from customer premises to the Internet. Customer premises are not just corporate sites but include, in selected geographic markets, consumer homes.

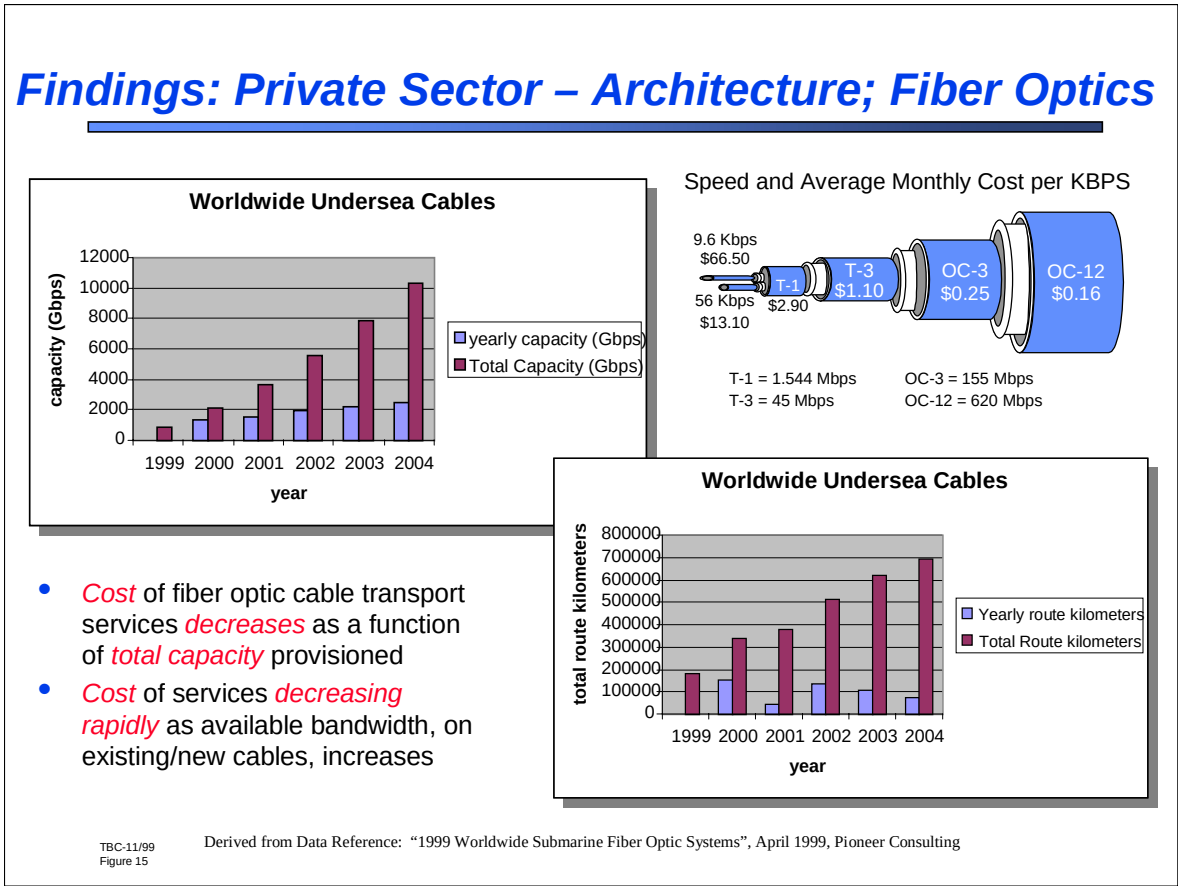
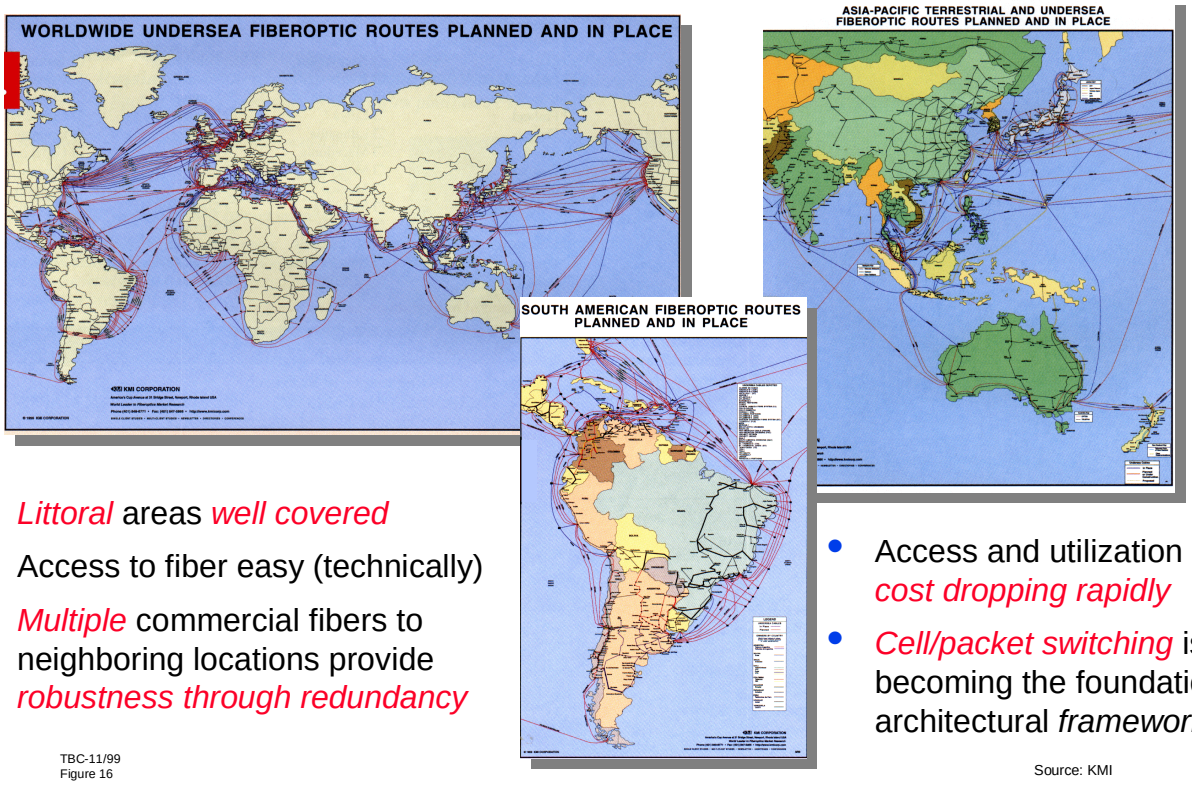


Figure 15 provides the data on the projected fiber-optic cable deployment worldwide over the next four years. As noted, the deployment rate is growing exponentially year by year, with an expected total of 700,000 route kilometers by 2004 and a total capacity of 10,000 Gbps. As this infrastructure is deployed, the cost of service to the user and consumer continues to decrease. Furthermore, as more of the media is shared through networking, the efficiency of use increases and the attendant cost of use charged to any single user decreases. This trend of increased capacity and reduced usage costs is expected to continue unabated over the next decade.

Findings: Private Sector – Architecture; Fiber Optics



- *Littoral* areas *well covered*
- Access to fiber easy (technically)
- *Multiple* commercial fibers to neighboring locations provide *robustness through redundancy*

- Access and utilization *cost dropping rapidly*
- *Cell/packet switching* is becoming the foundation architectural *framework*

TBC-11/99
Figure 16

Source: KMI

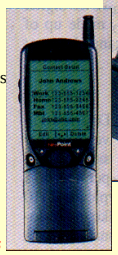
The sequence of maps in Figure 16 shows the distribution of undersea fiber optic systems throughout the world. The important points to note are the large number of systems deployed in 1999 and the number of landing points or access points to this system of networks. The geographic dispersion of the fiber-optic networks across different oceans and to many landing points, implies that it would be difficult, operationally and politically, for anyone to eliminate all undersea telecommunications systems without exceptional effort. The large number of landing points implies that one can gain access to this system of networks from most littoral regions.

It is also interesting to note that this cable is being deployed worldwide, both transoceanically and transcontinentally. As shown in Figure 16, the transoceanic cables will terminate in the littoral areas where worldwide population centers are projected to continue to grow. Similar market intelligence data for land-based fiber deployment show similar growth worldwide.

Findings: Private Sector – Architecture; Going Mobile

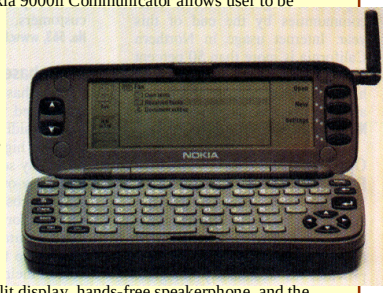
NeoPoint 1000

It's a phone, an Internet MiniBrowser, and PDA in one. The NeoPoint 1000, from Innovative Global Solutions (www.igsolution.com), is a CDMA digital phone that works on 1.9 GHz PCS networks (such as Sprint PCS) and has been garnering cooing sounds since it first made the cover of the *New York Times'* "Circuits" section. This very smart gadget with the cute face offers an amazing array of data and PDA functions, including smooth instant syncing to programs like Outlook, ACT! And Lotus Organizer. It's even got *speech recognition* functions that let you say things like "Internet, Stocks, Lucent" and it will bring up the Lucent stock quote on its screen. NeoPoint's "information alerts" will be especially attractive to corporate MIS – information alerts come through NeoPoint's Personal InBox that *captures e-mail, voice mail, and text messages.* All this and more for under $300.



Nokia 9000il Communicator

By fully integrating a GSM 1900 digital phone, a personal organizer, fax capabilities, data and messaging services, as well as Internet access into one compact device, the Nokia 9000il Communicator allows user to be fully connected and get Things done regardless of their location. The Nokia 9000il Communicator can quickly and easily sync up with standard POC-based calendar programs and other applications, and also allows users to connect to a company's network *to check information* in company databases or *download e-email*. The Communicator offers a backlit display, hands-free speakerphone, and the ability to conference call with up to six people. For more information, visit www.nokia.com



Qualcomm PdQ Smartphone

The PdQ smartphone combines CDMA digital wireless phone technology with the Palmpilot PDA electronic organizer into one device. The PdQ is a dual band/dual mode device that *supports Web browsing*. The device also supports Short messaging service, and will allow users to *send and receive e-mail, and wireless fax*. Users can input data using the Graffiti® power-writing software or the on screen keyboard. Users can store and retrieve addresses and dates within the address + date book within the PdQ.

And Many More!

The Internet user is going mobile at the platform and customer level

TBC-11/99
Figure 17

The fiber infrastructure is fixed and is supporting *in-situ* Internet use—the consumer, however, wants Internet services while mobile and untethered. The IT industry is addressing this need by integrating Personal Digital Assistants (PDAs) and like devices with PCS wireless devices. A few of these devices are shown in Figure 17. An important capability shared by these mobile Internet devices is the delivery of multimedia Internet information services to users on the move.

In support of these mobile PDAs, commercial mobile communications systems are quickly evolving toward their third generation. Analog cellular service (Advanced Mobile Phone Service - [AMPS]) dates from an early conception by AT&T in 1971 and was first deployed in 1983. Current PCS systems were initially developed and deployed in the mid-1990s, fifteen years after the introduction of AMPS technology. Standards bodies and telecommunications service providers are actively discussing third-generation PCS to be introduced in the next few years, a span of only approximately five to seven years since the introduction of second-generation PCS. Thus, the private sector is on a path to develop and deploy entirely new mobile telecommunications systems in less than a decade. This rate of innovation is expected to increase. Furthermore, the private-sector deployment strategy accepts the replacement of existing systems when market demand warrants. That is, the private sector is willing to leave old

systems behind and forge forward with new systems with increased capabilities.* However, mobile phones will continue to work in the worldwide telephony architecture and will increasingly work in the Internet architecture.

Mobile-device Internet services providers are anticipating the demand for exchanging information, voice, and fax to users on the move. Slow-scan video to and from hand-held Internet devices supported by third-generation PCS are already in research and development, with products expected in the marketplace within the next two years.

IEEE Spectrum, August 1999, pp. 20–28.

Findings: Private Sector – Architecture; Example Emerging Satellite Systems

System	Class	IOC Date	Min. Terminal Antenna Dia (m)	MRC Capacity (Mbps)*	2 MTW Capacity (Mbps)**	Total Cost	$/bps (2 MTW)
ICO	Narrowband MEO	2000	whip	9.3	186.8	2300	$12.31/bps
Iridium	Narrowband LEO	1998	whip	0.2	10.8	4500	$416.67/bps
Globalstar	Narrowband LEO	1999	whip	20	40	3200	$80.00/bps
Inmarsat F3	Narrowband GEO	1996	whip	42.5	85	1983.6	$23.34/bps
Intelsat 8	Wideband GEO	1997	2.4	2376	4752	2559	$0.54/bps
Italsat	Wideband GEO-Data	1996	1.8	222	1920	2188	$1.14/bps
Astrolink	Wideband GEO Data	2002	1.8	225	2000	3830	$1.92/bps
Spaceway	Wideband GEO-Data	2003	1.8	225	2000	3390	$1.70/bps
@Contact	Wideband MEO-Data	2003	1	275	4000	3600	$0.90/bps
Spaceway NGSO	Wideband MEO-Data	2004	1	1440	4000	2400	$0.60/bps
Teledesic	Wideband LEO-Data	2003	0.7	1035	11500	12000	$1.04/bps
Skybridge	Wideband LEO-Data	2002	0.7	2500	20000	4200	$0.21/bps

TBC-11/99
Figure 18

* MRC geographic region = 320 km diameter
** MTW geographic region = 3200 km diameter

- Average capacity**/cost of Wideband System is 6 Gbps for $3.3B *($0.54/bps)*
- Average capacity**/cost of Mobile System is 100 Mbps for *$2.5B ($24/bps)*
- Growing number of former *senior DoD persons* in senior positions in *private sector* SatCom companies

In addition to PCS-based wireless Internet services, the private sector telecommunications industry is planning to respond to the consumers' needs for wireless Internet services by providing a space-based wireless telecommunication infrastructure. In addition to supporting narrowband mobile services, several satellite systems are being planned to support broadband services to both fixed and mobile subscriber nodes. Figure 18 provides a summary of several systems that are already deployed or are planned for deployment over the next three to four years.

The diversity of the systems listed is great, in the number of spacecraft in each system, the service to be supported by each system, the ground segment needed for each systems (both control and user infrastructure), the capacity of each system, and the like, thus making it difficult to compare these systems. The Task Force chose, for illustrative purposes, to capture the information noted in the table. A mixture of GEO, medium earth orbiting (MEO) and LEO systems is included. Where a GEO system is indicated, the Task Force assumes that four satellites would be used to ensure global coverage. For the purposes of comparison, a major regional conflict (MRC) is defined as a conflict involving an area equal in size to the Korean Peninsula. A major theater of war (MTW) is defined as a region one hundred times larger in area than an MRC, and two MTWs are assumed to be non-overlapping. For most systems shown in Figure 18, the beam coverage area of a satellite is equal to or larger than the MRC area; consequently, the MTW capacity makes better use of the full system capacity.

Conventional relay satellites are represented by the Intelsat 8 entry in Figure 18. These systems are relatively inexpensive, due to their simple design, mass production, and modest ground terminals. They provide high capacity for an MRC but only modest capacity for two MTW operations, compared to the other systems noted in the figure. Italsat is a spot beam system with on-board switching. Inmarsat supports mobile users. The others are emerging systems. These systems include Astrolink, Spaceway, @Contact, Teledesic, and Skybridge, which are intended to support fixed-site, broadband data telecommunication requirements. ICO, Iridium, and Globalstar illustrate the emerging systems intended to support mobile-user voice and data services.

Data are included in Figure 18 to show an expected initial operational capability (IOC) date for the emerging systems. Several of theses systems are still in the regulatory approval stage and will require some time before IOC is achieved. In addition, Figure 18 provides information for each system on minimum user terminal antenna size in order to provide an indication of the complexity of the users infrastructure for each. Systems that support a range of data rates will usually require a larger antenna than the minimum size noted to operate at high rates.

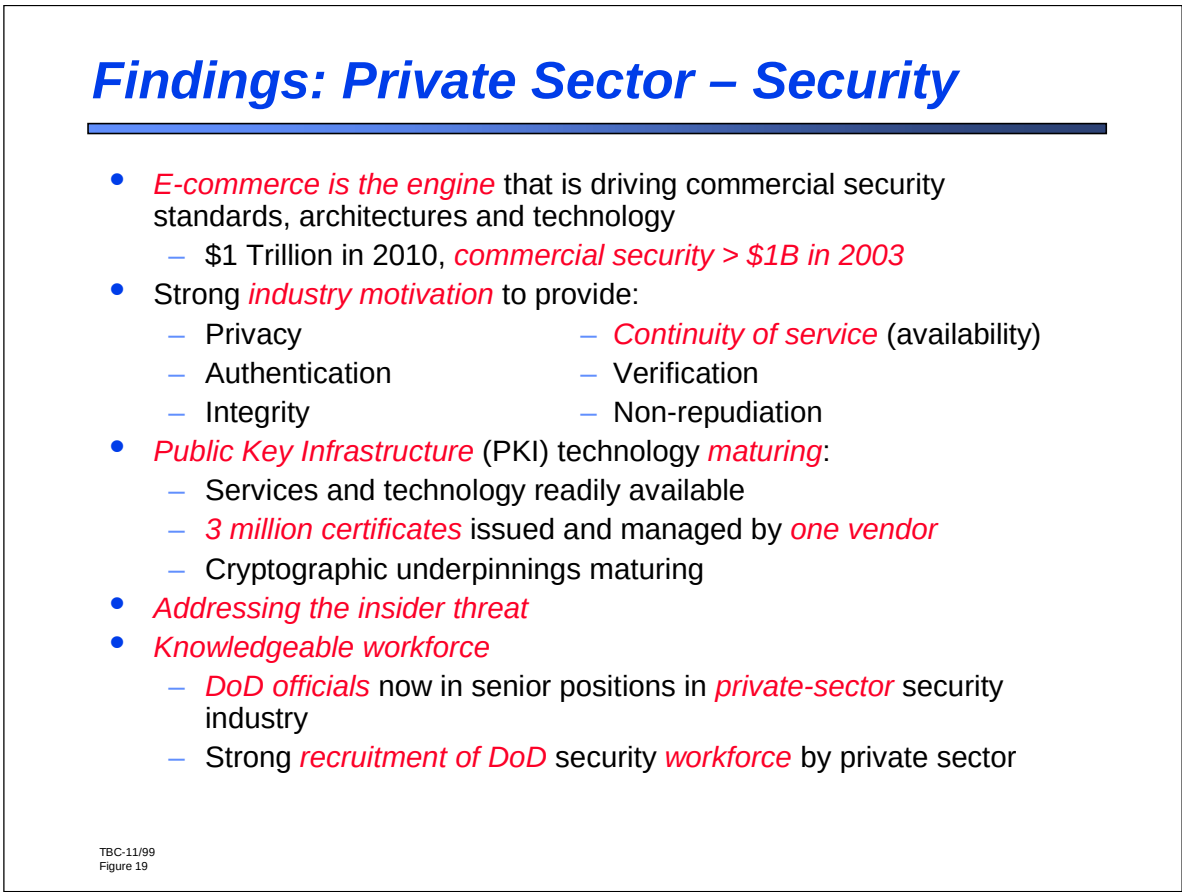
An important parameter listed in Figure 18 is estimated system costs, which include a number of elements.

- Non-recurring Engineering (NRE) costs for the development of the systems and the space vehicle
- The cost of the space vehicle production
- The launch costs, which depend upon the orbit and the vehicle weight
- The ground infrastructure costs for teleports or gateways
- Maintenance costs to operate the system and the infrastructure over the lifetime of the system.

In the last column of Figure 18, costs are normalized on a cost per bit per second (bps) of capacity that can be delivered by each system into two nonoverlapping MTWs. These prices reflect the ownership of the systems. For comparison, the system must be used for an application that consumes all of its capacity. As an alternative to acquiring the entire system, system capacity might be acquired by purchasing services. The cost per bit under these circumstances changes because transferred bulk data is being purchased rather than capacity. For example, if Globalstar service costs $1.50/minute at 9600 baud, *bulk data transfer* is being purchased at $2.60/Mbit. If a Globalstar system is purchased and used for a two-MTW application, *capacity* is being purchased at $80/bps. Long-term leases of capacity can be negotiated but associated costs are typically comparable to those of ownership. Lease costs are higher than ownership costs if short-term leases are used. The use of short-term leases or bulk data transfer may be attractive for “surge” capacity if they can be procured on a non-preemptive basis.

It is interesting to note from Figure 18 that most systems have comparable total costs but the mobile systems have far less total capacity since they are optimized for low and medium rate operation to low-power, small user terminals. For two MTW operations, the wideband fixed-site systems average $0.54/bps and the narrowband mobile systems average $24/bps.

It should also be noted that the emerging satellite systems that seek to support data services expect to be integrated into the Internet. In some cases these systems are positioning themselves as a network within the network-of-networks framework of the Internet. These systems will support IP packet switching and routing. Other systems view themselves as providing trunking (link/backbone) facilities as bypass services to fiber-optic cable in the Internet. In all cases, these systems will be integrated into the Internet.



As noted earlier, the engine driving the expansion of the Internet is e-commerce. The deployment of fiber-optic cable, the introduction and integration of space-based telecommunication systems into the Internet, and the introduction of wireless PDA devices for mobile Internet services are all attempts to meet the e-commerce market demand. Recent reports developed by the Department of Commerce indicate that 35 percent of the nation's real economic growth from 1995 to 1998 came from the IT business sector. Industry is becoming aware that any threat to the reliability, security, and availability of the Internet poses potential threats to the delivery of services to the American public as well as to the economic health of our nation and other nations around the world.

The enormous incentive for industry to provide privacy, authentication, data integrity, quality and continuity of service, verification, and nonrepudiation is being satisfied, in part, through the rapidly maturing Public Key Infrastructure (PKI) technology. PKI services and technology are now readily available. For example, one private sector company, during their briefing to the Task Force, cited the fact they are holding and managing 3 million certificates. The Task Force was also informed that private sector market demand for immediate revocation of certificates, and notification therefore, is being developed and will be available within the next year. Thus, on an e-commerce transaction-by-transaction basis, a users' certificate will be

checked and the transaction approved based on the real-time verification of the users' "qualifications" for engaging in the transaction.

Similarly, significant progress has been made in deploying intrusion-detection systems (IDSs). The private sector has begun focusing on two methodologies: host-based products to guard operating systems, web servers, and databases; and networked-based intrusion detection products that work by scanning network traffic to detect suspicious traffic anomalies. In the private sector, one company, with its Intruder Alert product, has captured three quarters of the host-based market segment. In a similar fashion, another company holds about one half of the network-based market with its product. According to International Data Corporation (IDC), the intrusion detection market has grown from about $20 Million in 1997 to about $100 Million in 1999 and is expected to reach, by itself, $528 Million by 2005. In the 2004 timeframe, the *total* Internet security market is expected to reach $1 Billion.

It is interesting to note that while e-commerce is the forcing function for the rapidly growing Internet security investments, the leadership of this private-sector industry is coming from, in part, from prior DoD senior employees. In many cases, these individuals are merging their understanding of security needs and practices within DoD with the needs of the private sector. This indirect merging of the security needs of the two sectors is a potential opportunity for DoD to leverage and influence this emerging Internet security industry in a manner that will allow for technology to be effectively used by DoD.

Findings: Private Sector – Security

- Other Internet security *technologies readily available*
  - IPsec (IP Security)
  - PGP (Pretty Good Privacy)
  - DoD-certified trusted guards
  - SSL (Secure Socket Layer Services)
- *Transport* layer and *network management* being *secured*
  - IPsec between routers (based on certificates)
  - Secure Network Management (S-SNMP)
  - Network encryptors commercially available (ATM, EtherNet)
- *Secure multimedia* service technology evolving
  - SMIME (Secure Multipurpose Internet Mail Extension)
  - Available today - other technology will evolve as demands arise
- *Standards-based security architecture* being promoted
  - *"Defense in Depth"* framework
  - Common Data Security Architecture *(CDSA)* published by Open Group
  - CDSA-based middleware (version 1.2) available
  - *Software integrity* concerns being addressed
  - *Multiple levels* of security supported

TBC-11/99
Figure 20

In addition, to the security technologies noted in Figure 20, the private sector is developing a broad spectrum of other security technologies for the Internet. Examples are Internet Protocol security (IPsec), Pretty Good Privacy (PGP), Secure Socket Layer (SSL), and DoD-certified trusted guards, to name a few.

In addition to providing end-to-end application security, industry is also focusing on securing the transport layer of the Internet using IPSec, Secure Simple Network Management Protocol (SSNMP), network encryptors for ATM, Ethernet, Frame Relay and other related technologies. Furthermore, the Internet Engineering Task Force (IETF) has been very active in establishing standards to secure the Internet switching fabric. The next generation of SNMP, SNMPv3, will include enhancements to support more robust key exchange mechanisms between network administration and managed devices, thus permitting secure network management and administration.

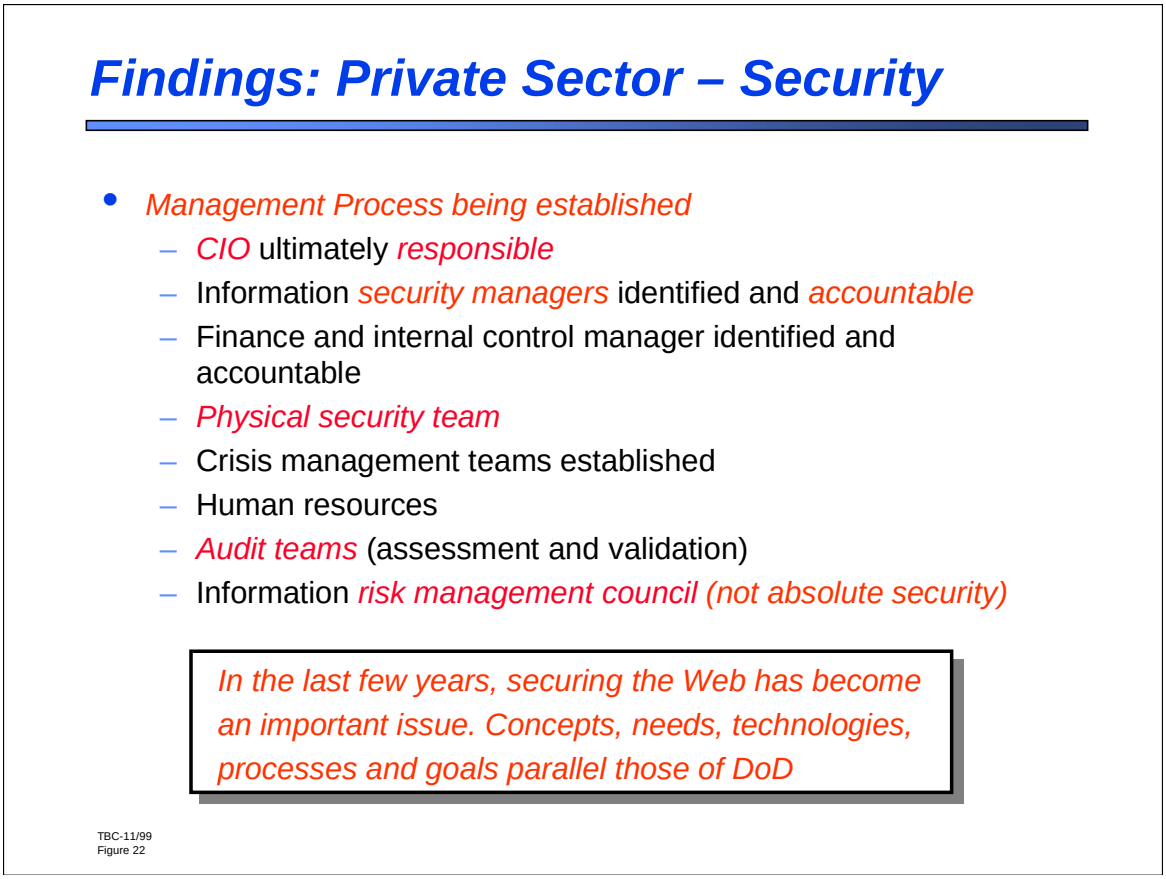
With the growth in the Internet security industry, and the resulting growth in the number of security technologies, the need for a standards-based security architecture is emerging. In response to this need, the Open Group has spearheaded an initiative to codify and publish an industrywide, open security architecture for the Internet. This architecture, called the Common Data Security Architecture (CDSA), has been released and has now been implemented by Intel and IBM. The architecture, and the middleware implemented to date by these two

companies, supports a defense-in-depth strategy and multiple levels of security, and will address application software integrity by checking that hosted software is “certified” (through PKI certificates) to be authentic and unmodified.

An important shift in philosophy is also occurring in the private-sector security marketplace. Industry and consumers alike are coming to the realization that security architectures and technologies, while necessary, are insufficient to ensure secure e-commerce on the Internet. An understanding is emerging that a comprehensive framework is also necessary—a framework that sets security policy and processes in place for on-line enterprises, establishes a communication strategy to ensure that within an enterprise these policies, practices, and processes are clearly understood by all employees, and sets processes to ensure that the enterprise Intranet infrastructure and security practices are continuously audited.

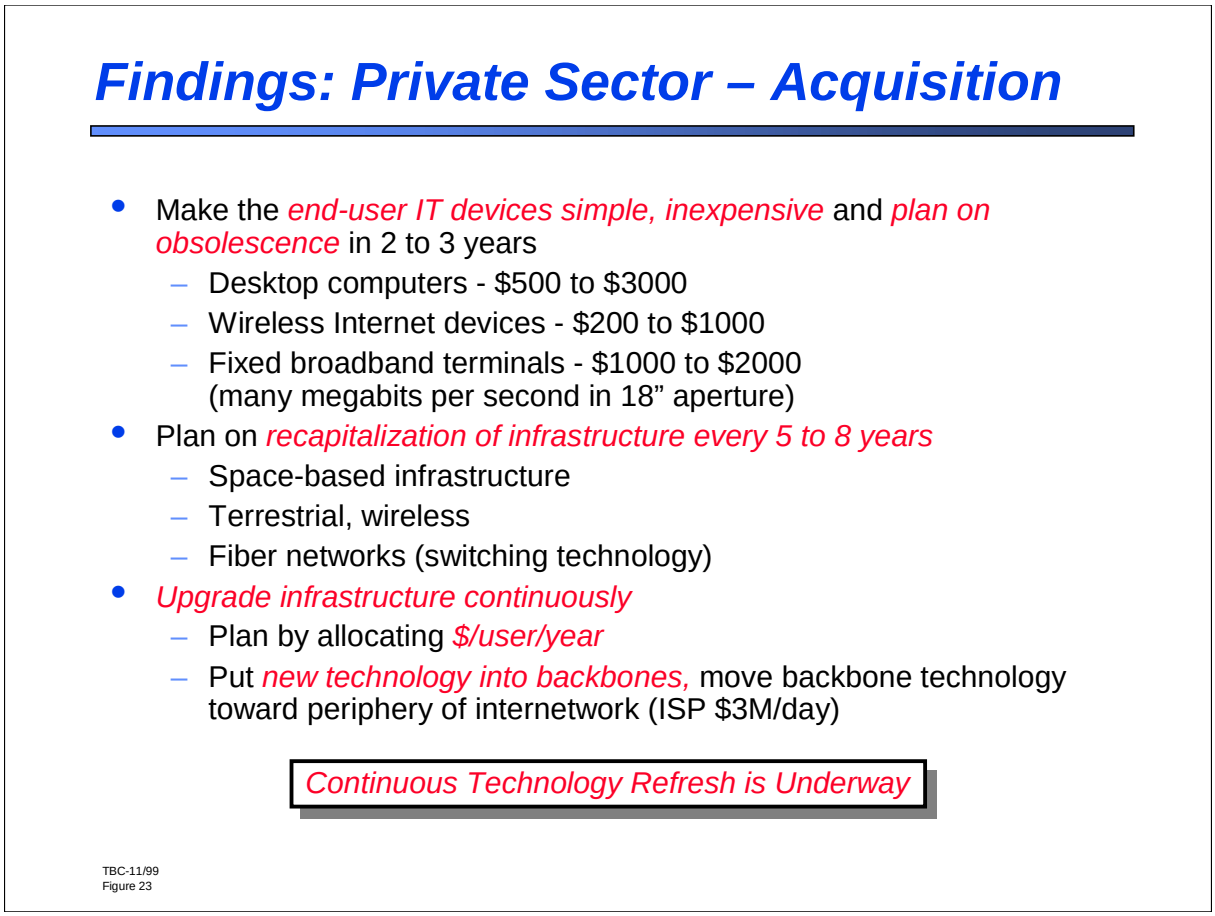
Enterprises are beginning to formulate corporate information security policies that cover information creation, use, transfer, and destruction (electronic and/or physical). In addition, physical security and access controls are beginning to be enforced, internal access to corporate information systems is being controlled and access to corporate databases being granted on an as required basis. Through the use of PKI, multiple levels of security and access control are being implemented. Employees are being granted access to only the corporate information that they need to be able to meet their responsibilities.

Commensurately with the emerging establishment of policy and processes, enterprises have begun to implement user training on security tools, techniques, and responsibilities. Training for compliance with policy and procedures is expected and enforced because of the growing realization that an enterprise's intellectual property, market strategy, and financial position in the marketplace are critical information that, if jeopardized, could affect the future viability of the organization.



As indicated in Figure 22, the private sector is also realizing that its security framework must also include accountability. Today, industry empowers a single individual within an enterprise with overall responsibility for domain or corporate security. The Chief Information Officer (CIO) or equivalent is that single individual. In turn, the CIO holds each of an enterprise's information security managers accountable and so on down the chain.

Through briefings received, the Task Force became aware of private-sector service organizations that will help an enterprise establish its security framework (policy, processes, and accountability) and help the enterprise establish Red Teams and Information Risk Management Councils. These service companies help an enterprise establish and maintain its security policy; and the service organizations will also monitor, test, and evaluate the implementation and maintenance of the policy to ensure that it is adhered to and is effective.

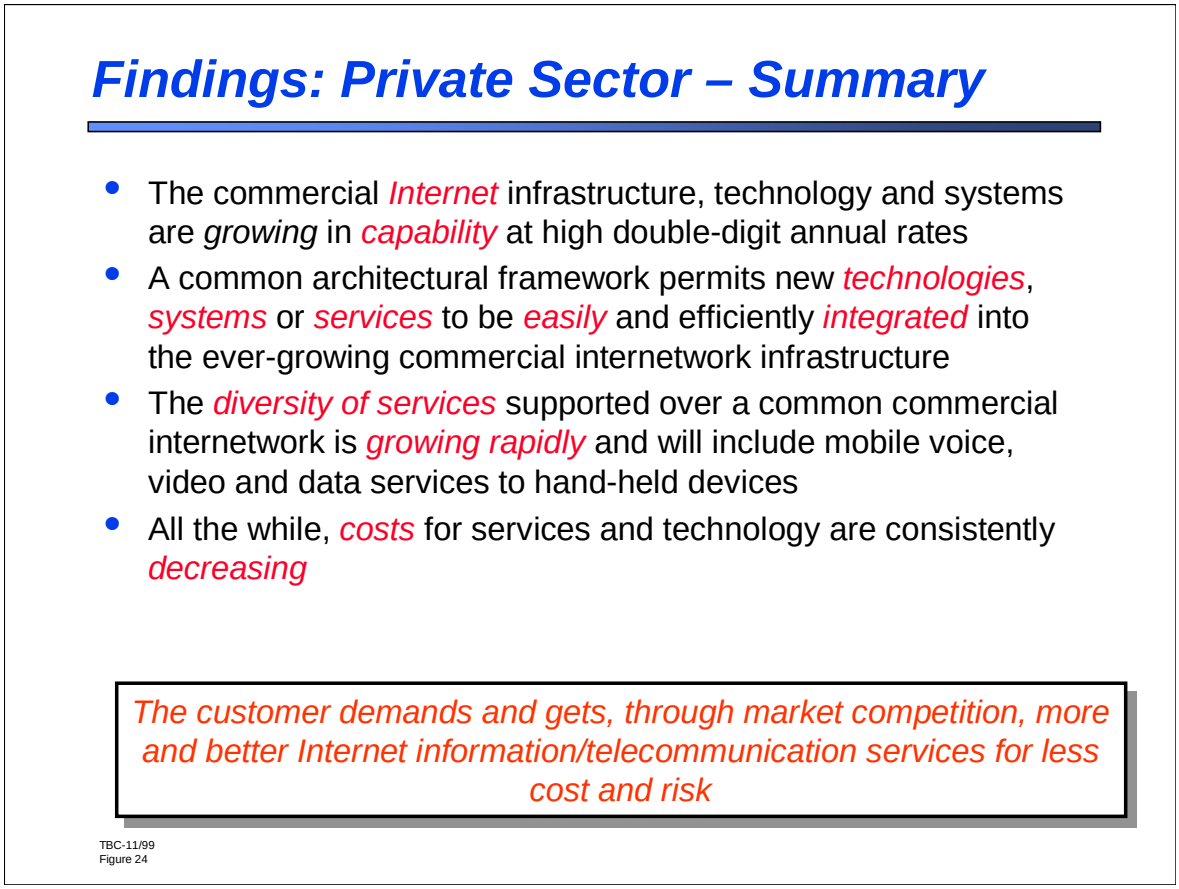


As the Internet continues to position itself as a critical element of our national economy, and the global economy as well, it is clear that demand for secure information services and increased transport capacity will continue to grow at very dramatic rates. The implication of this growth is the continued introduction of new technologies into the Internet that in turn will require substantial recapitalization of the infrastructure.

The private sector has responded to this demand by developing an acquisition strategy that focuses on two different segments: the customer's equipment and the service-providers' transport infrastructure. End-user equipment is designed to be simple and low-cost, and is expected to be replaced every two to three years. Short turnover intervals mean that new features and capabilities continually are brought into service. Service providers (e.g., telecommunications companies and satellite services companies) plan to recapitalize their infrastructure every five to eight years. Furthermore, the new system is not necessarily directly backward compatible with earlier systems. For example, near-future fiber-optic systems based on DWDM will not necessarily be directly compatible with systems deployed only seven to eight years ago. What has remained constant is the architectural framework and a core set of open-standards-based protocols that permit the integration of these new technologies into the Internet.

Thus, the private sector acquisition strategy is the continuous updating of the infrastructure to meet anticipated market demand. As major Internet service provider described the situation to

the Task Force, “We invest $3 Million per day” for the introduction of new technology and, “at any point in time we have as much capacity on order as we have installed in the network.” Similarly, corporations plan to spend a fixed amount per staff member per year, on the order of $10,000, to provide their employees with suitable IT infrastructures. In both these cases, this capitalization expense is recaptured through fees for service and improved productivity, respectively. In either case, corporations want a substantial return on their investment.

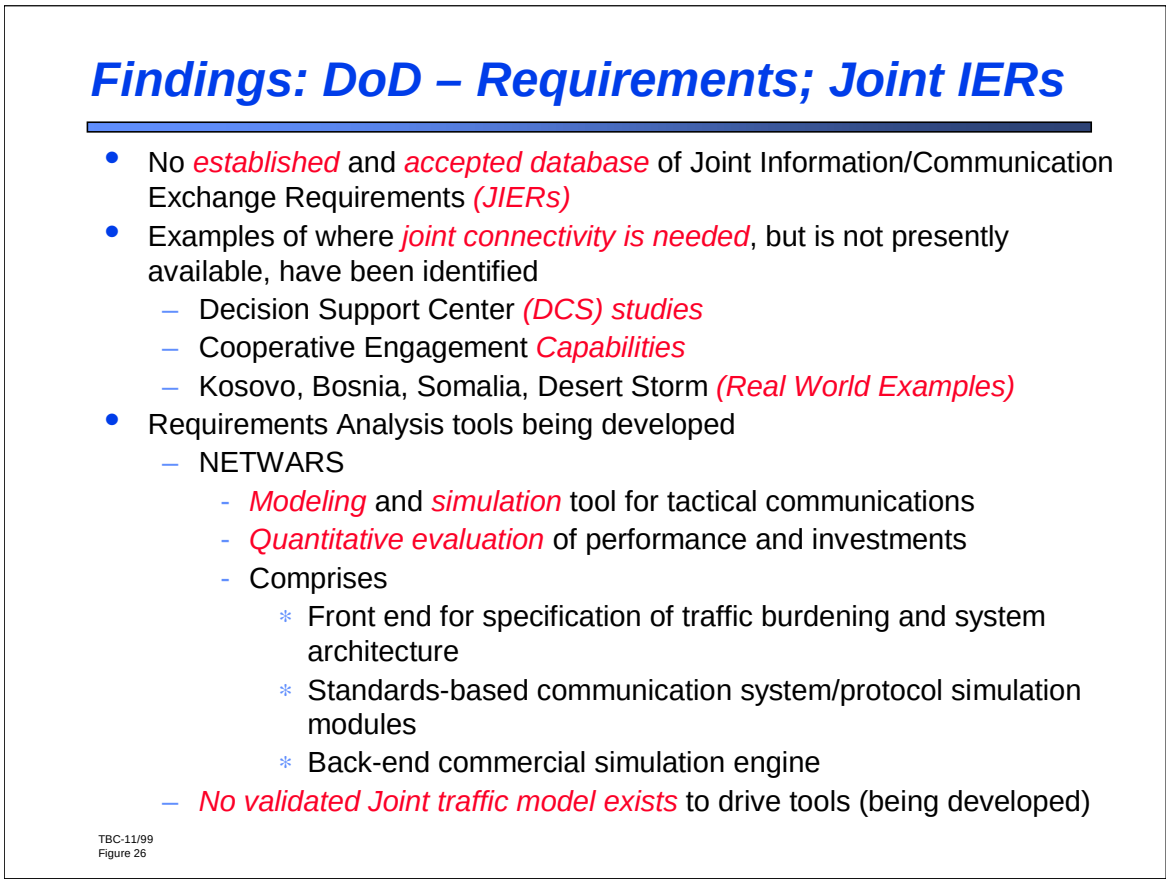


In summary, the Internet has, and will continue to, revolutionize the way business is conducted in the United States and the world in general. The demand for information services, the support for e-commerce, and the ability to dynamically form communities of users to address areas of common interest has motivated, and will continue to motivate, the development and introduction of new IT into the Internet at accelerated rates.

The introduction of these new technologies is facilitated by the well-understood architectural framework and the open standards and protocols that are at the foundation of the Internet. As these new technologies are introduced, new and innovative information services are provided to end-users: organization, people, sensors and actuators. These services and increased user comfort and sophistication on the Internet has stimulated and will continue to stimulate new ways of doing business and new ways for people to collaborate. The resulting business and societal reengineering will result in greater well-being for our nation and the global community.

Department of Defense Findings

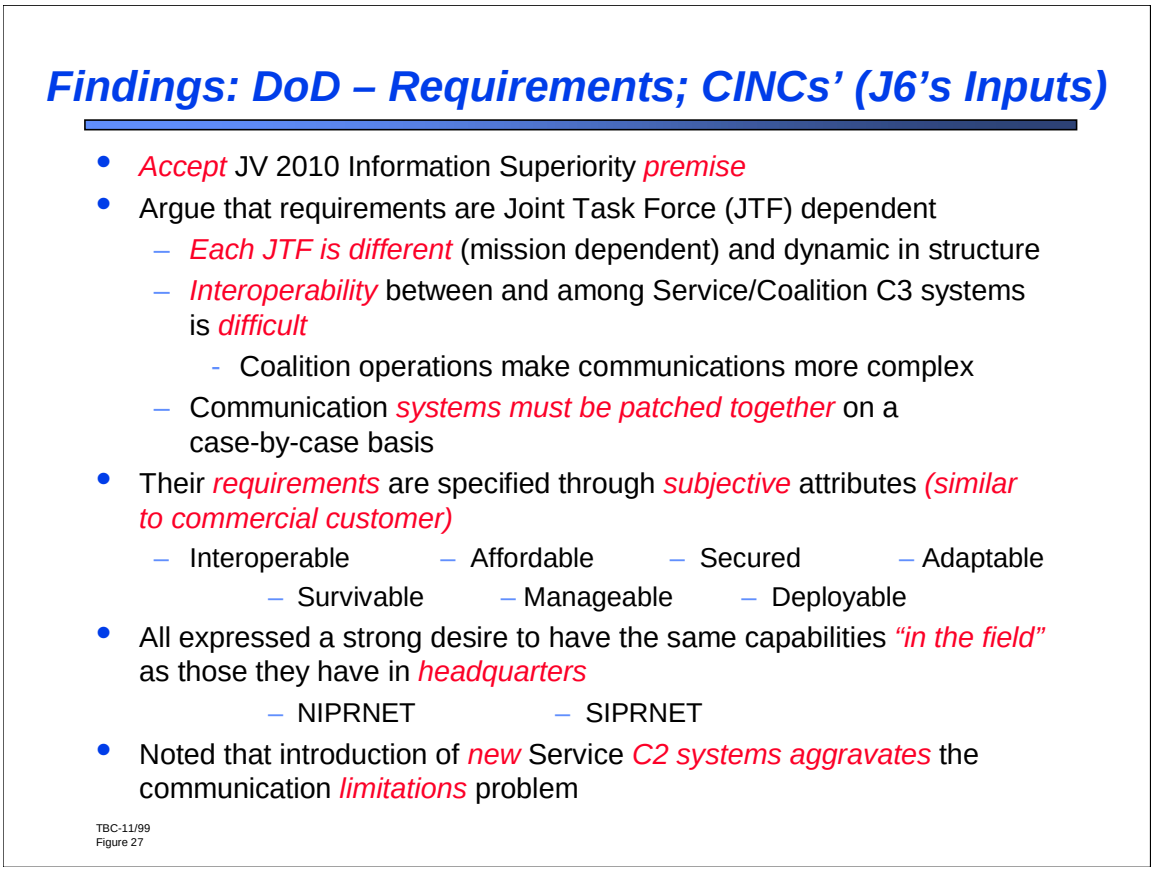
TBC-11/99
Figure 25



As a result of the briefings presented to the Task Force and through subsequent analyses, the group observed that there are no established or accepted DoD Joint Information Exchange Requirements (JIER) databases. Clear examples were cited by DoD briefers of areas where joint connectivity would be needed, but is currently not available. Examples presented to the Task Force included sensor-to-shooter studies from the Decision Support Center (DSC), tactical data exchange assessments for Cooperative Engagement Capabilities (CEC), and real-world examples from Kosovo, Bosnia, Somalia, and Operation Desert Storm.

The Task Force also observed that there are no DoD-wide "accepted" requirement analysis tools. There are several being developed, the most promising one is the Network Warfare Simulation (NETWARS) model, under J6 sponsorship. NETWARS is based on the commercially available network simulation system called Operations Network (OPNET). OPNET models both the statistical nature of a network (nodes, traffic distributions) and the characteristics of telecommunication links and the protocols used in the networks that are modeled. Once NETWARS is completed, it will allow quantitative evaluations of performance and the value of investments associated with planned or recommended tactical telecommunication networks for CINC, Service, Joint Staff, and DoD users. It will enable traffic burdening and system architecture analyses for various tactical communication systems and the evaluation of emerging technologies, and it will enable the military planners to perform "what if" communication system trade-off analyses.

The Military Communications Electronics Board (MCEB) has endorsed NETWARS as a Joint and Services communication-modeling tool. It is imperative that a JIER database for several representative joint force structures and corresponding mission scenarios be developed for NETWARS through active participation by the CINCs and the military Services. Such databases would permit the DoD to assess the value of acquiring a specific (tele)communication system to resolve capacity limitations in our DoD infrastructure and, equally important, the databases would facilitate the assessment of the value of internetworking the many DoD communication systems into a DoD-wide virtual Intranet similar in architecture to the private-sector Internet.

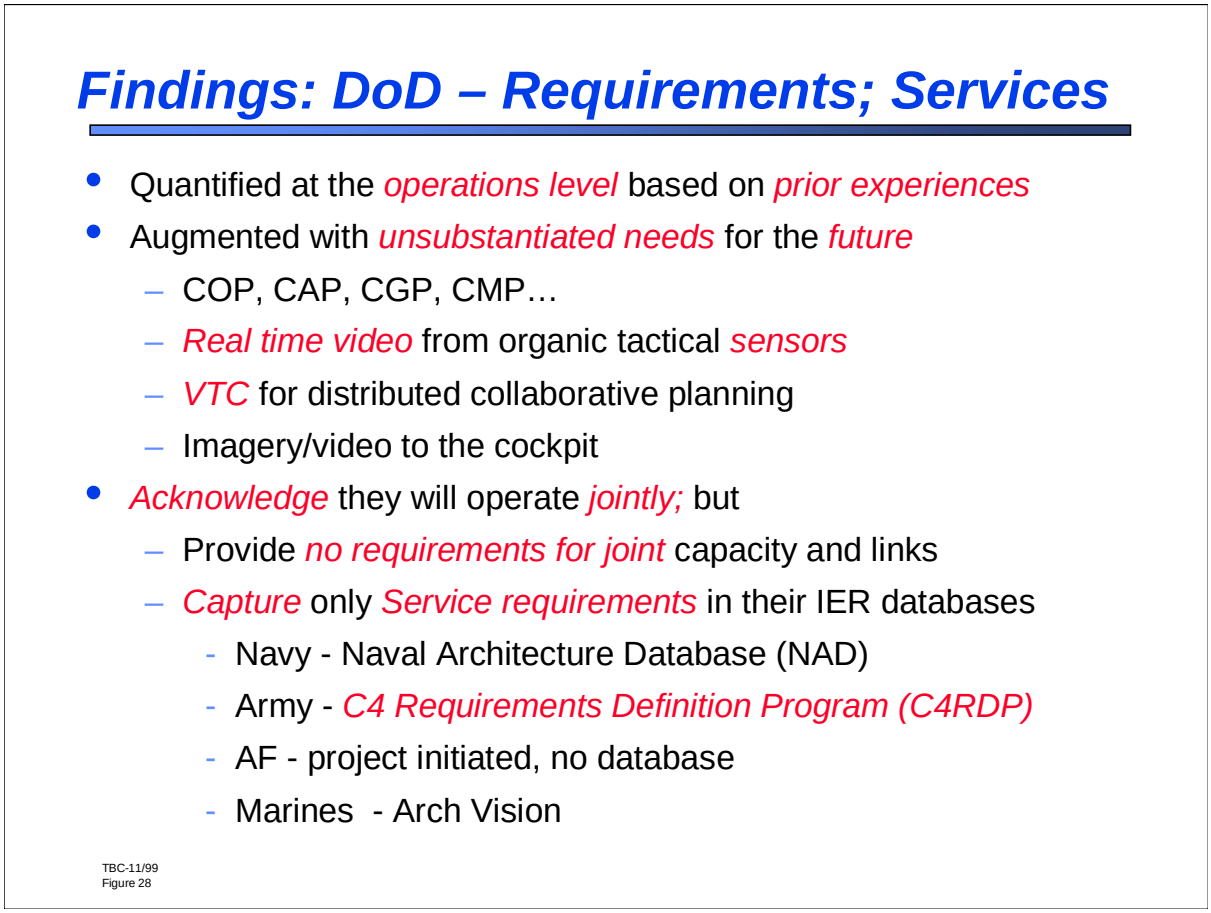


As part of the Task Force's fact-finding efforts in joint communications requirements, the panel invited the CINCs to brief on their needs. From the briefings provided, the following observations were made: First, the CINCs accept and endorse the JV2010 premise that information superiority is the key enabler for dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. Second, the CINCs' requirements are JTF dependent; they recognize that each JTF is mission dependent and dynamic in structure. They argued that the telecommunications infrastructure supporting JTFs must be flexible, to allow the simple, efficient tailoring of the infrastructure for different missions and force structures. Third, the CINCs stated that interoperability between and among Services' Command and Control (C2) systems is difficult, from the CINCs' perspective. They emphasized that Service communication systems are not interoperable and provided several examples where interface patches had to be implemented to allow information to flow between the different Service systems. The CINCs' input is summarized in Figure 27.

The JTF communications requirements could not quantified by the CINCs, but they did express their needs much as the commercial consumers do: they cited subjective attributes such as interoperability, affordability, adaptability, manageability, deployability, securability, and survivability. They wanted (needed) their communication systems to be "better, faster, and cheaper," a clear analogy to the expressed needs of the commercial customer.

Further, all CINCs expressed a strong desire to have the same capabilities in the field as those they have in their headquarters; very specifically, NIPRNET and SIPRNET information services, reinforcing from a CINC's perspective, the need for a DoD-wide virtual Intranet, as opposed to thinking about tactical, strategic and post-camp-station telecommunication and information services as separate entities.

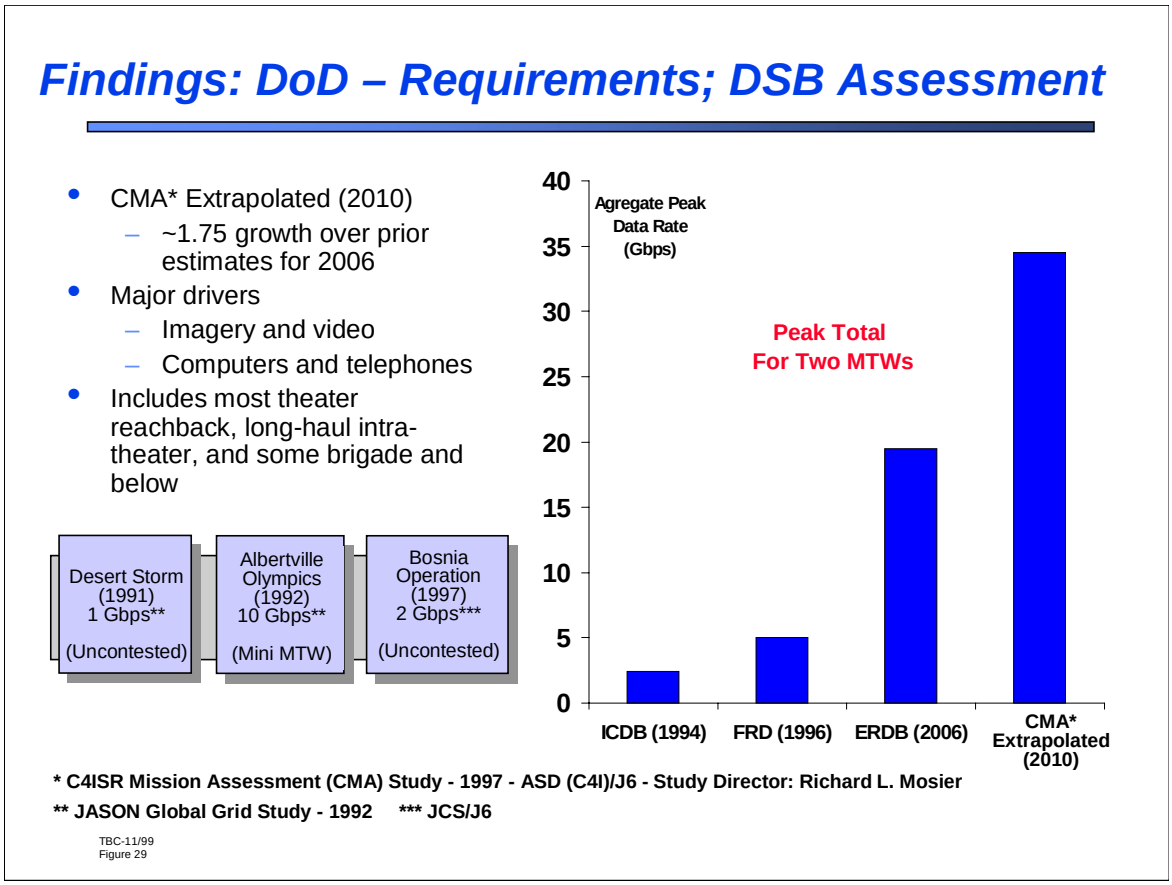
Finally, the CINC's representatives noted that as new Service and Joint C2 systems are introduced, greater capacity and performance demands are placed on the existing Service communication systems. They expressed a concern that these C2 systems provide more information that must be (should be) shared in a joint environment. The already limited communication system capacity is further stressed by these demands.



Following discussions with the CINCs, the Task Force asked that the Services brief on their communication requirements—both from their own and from a joint-warfighting perspective. The Services discussed their requirements in the context of the Army 2010, Navy Operational Maneuver from the Sea, Air Force Expeditionary Force, and Marine Corps Extended Littoral Battlespace. It was acknowledged by the Services that their vision of operations is shifting from platform-centric to network-centric warfare; nonetheless, the Services' requirements, when quantified, were only at platform or operations facility (OPFAC) levels. These requirements were formulated in the context of prior "circuit-based" requirements and unsubstantiated needs for additional application services in the future, such as the Common Operational Picture (COP), Common Air Picture (CAP) Common Ground Picture (CGP), and Common Maritime Picture (CMP). Other future needs, such as real-time video from organic tactical sensors, video teleconference (VTC) for distributed collaborative planning, and imagery and video to the cockpit, were discussed only in subjective terms.

The Services acknowledge that they will operate jointly, but could not provide any requirements for joint telecommunication capacity and links—only a Service-centric view of their requirements was presented to the Task Force. They did capture their telecommunication requirements in databases such as the Naval Architecture Database (NAD), the Army's C4

Requirements Definition Program (C4RDP) database, and the Marines' Arch Vision database. At the time of this review, the Task Force observed that the C4RDP was the only one that specifically called out information exchange requirements (IERs) with sufficient specificity and rigor to allow the analysis of telecommunication-system performance and requirements with a tool such as NETWARS.



Given the lack of specific, hard data on Joint or Service present and future JIERs, the Task Force undertook the challenge of trying to estimate what the total aggregate peak telecommunications capacity might be required for 2 MTWs in the 2010 time frame. As noted in Figure 29, the Task Force formulated this estimate based on the findings of prior DoD studies, recent real world experiences in both the DoD and private sectors and on estimated growth of information flows in military operations resulting from the introduction of new C2 and tactical ISR systems.

Prior studies reviewed by the Task Force included the following. In 1994, the JCS-validated Integrated Communications Database (ICD) indicated a worldwide peak requirement for a total of approximately 2.5 Gbps for 2 MTWs. This database viewed telecommunication systems as circuits with many of the requirements being expressed as dedicated links with an associated data rate. This database captured requirements that were typically served by military satellites and leased commercial, long-haul services (both satellite and terrestrial).

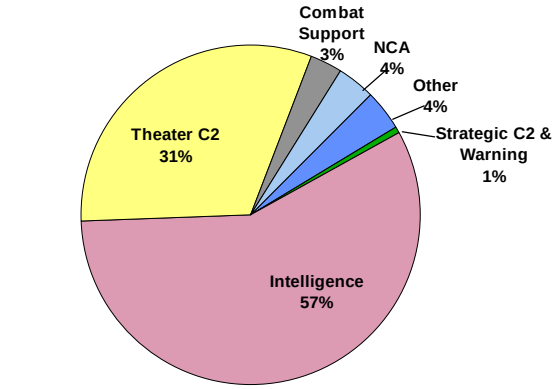
The Functional Requirements Description (FRD) study, completed in 1996, determined a peak need for 2 MTWs of approximately 5 Gbps, while the Communications Mix Study (CMA) completed in 1997 indicated that by 2006 the peak requirement would grow to approximately 20 Gbps. As with the previous studies, the CMA analyses were also based on

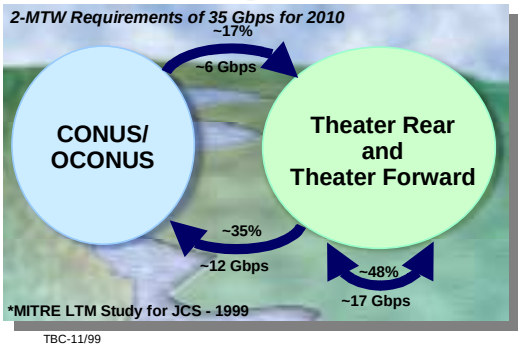
requirements expressed as equivalent “circuits” with specified capacities irrespective of usage duty cycles.

The CMA requirement included four categories: Hard Core, Core, Assured, and Routine. The Hard Core information exchange requirements were those needed to survive an extreme threat environment. Core requirements included those that are mission essential and urgent, where no interference is tolerable (e.g., call for Fire). The Assured requirements included those that are mission essential but not urgent, where temporary interference is tolerable (e.g., database updates to support deliberate planning). The fourth category, routine requirements, are mission essential, but significant delays can be tolerated (e.g., payroll). Although quantitative data is not available, the CMA study estimated that the Hard Core and Core requirements constitute approximately 25% of the total 2-MTW peak-capacity estimate of 20 Gbps. The CMA study also estimated that the Hard Core peak requirements ranged from 600 Mbps to 1 Gbps.

These previous studies have indicated a requirement growth of approximately 15% annually over the years covered by the studies. Based on this assumption, the Task Force forecasts, for 2010, a total peak DoD communication capacity requirement of 35 Gbps for 2 MTWs. The Task Force chose to be conservative in this estimate; in fact, a recent study for the J6 put the 2-MTW peak requirements at as high as 100 Gbps in the same time frame. Although the Task Force estimate is clearly a large number, there are several real-world benchmarks to support such an exponential increase in requirements. Operation Desert Storm (1 Gbps, JASON Global Grid study - 1992) and the NATO operations in Bosnia (JCS information, 2 Gbps), both widely viewed as “uncontested” operations, clearly highlight the growth of peak requirements. Further, it was observed that the peak telecommunications capacity needed for the 1992 Albertville Olympics in France has been estimated to be 10 Gbps (JASON Global Grid study – 1992), which this Task Force equates to a small theater of operations in a military context.

Findings: DoD – Requirements; DSB Assessment





TBC-11/99
Figure 30

- *Major* functional *driver* is *Tactical intelligence*
  - Imagery dissemination
  - Intel products for mission planning
- Theater C2 reflects the growing number of *C2 automation systems* along with increasing number of *"smart" weapons*
- *Emerging* needs for *Medical* and *Logistics* data could significantly increase the requirements

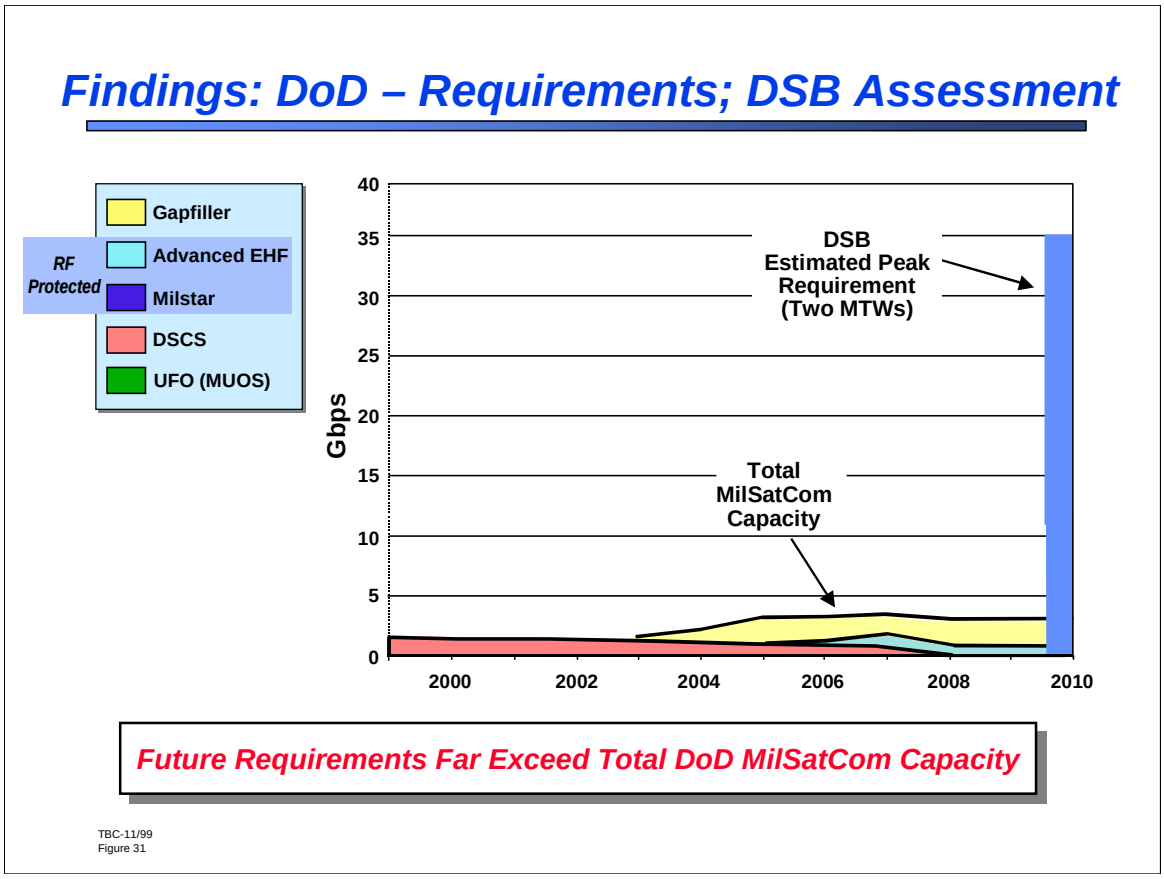
The 35 Gbps capacity needed for 2 MTWs supports several types of military information. The Task Force estimated, based on a 1996 DoD Satellite Communications (SatCom) Functional Requirements Description, that the major functional capacity driver is tactical intelligence, with a substantial fraction of this requirement attributable to imagery dissemination and distribution of Intelligence products to support mission planning. Theater C2 is the second largest consumer of telecommunications capacity, reflecting the growing number of C2 automation systems being deployed, along with the increasing number of "smart" weapons requiring substantial amounts of information for their employment. The Task Force noted that its estimated 35 Gbps requirement for 2 MTWs is conservative, given the anticipated needs emerging for medical and logistics data that will flow over the DoD telecommunications infrastructure. Although no specific data exists for these functional areas, the need to support JV2010's focused logistics vision and medical support for our warfighters in the field will result in traffic loads greater than those currently experienced or that the Task Force estimated for 2010.

Also, based on the results of the recent J6 study, it is anticipated that for 2010 about half of the total requirements will be intratheater, with the remaining between theater and CONUS/OCONUS. The Task Force believes that tactical intelligence (imagery) will constitute

35% of the remaining traffic and will be from theater to CONUS/OCONUS. It is recognized that traffic distribution is highly dependent on the future operational scenarios.

Although the aggregated peak traffic model derived by the Task Forces does not have a detailed JIER database to support it, the Task Force believes that the estimates are a conservative view of what the requirements are likely to be if 2 MTWs must be supported simultaneously, per our existing national security policy. The reason for generating and vetting this estimate with real-world examples is that an estimate is needed to meet the tasking provided in the TOR for the study. Given that no quantified DoD requirement for the future could be provided to the Task Force, the conservative estimate it derived allowed the panel to address its tasking.

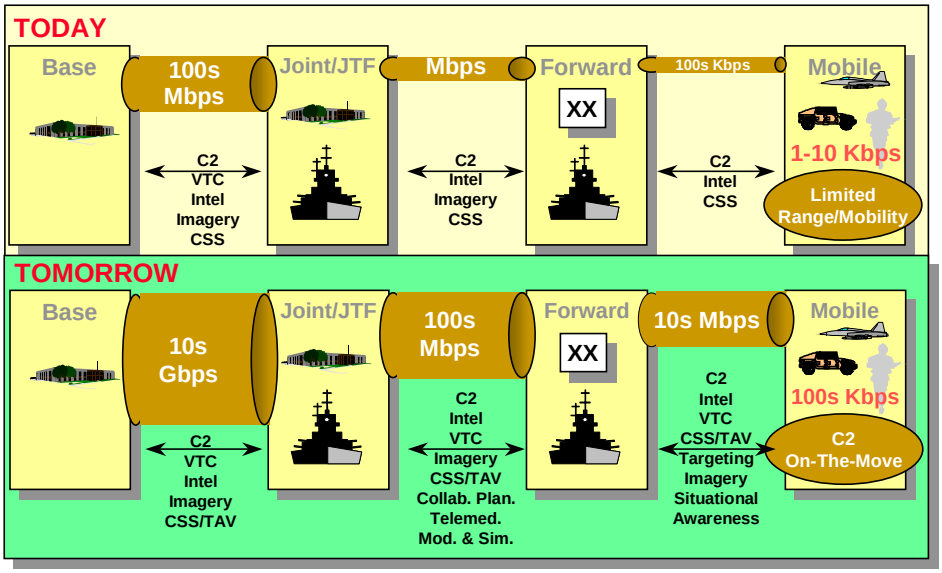
Based on the 35 Gbps estimate, corresponding estimates for peak communication capacities from 2 MTWs to CONUS (or other fixed sites) and vice versa, can be estimated from the Last Tactical Mile (LTM) study results that estimated the percentage of traffic flow between these geographic regions. These percentages are captured in Figure 30. The resulting peak capacities are 12.25 Gbps and 6 Gbps, respectively.



From briefings provided by the US Space Command, the Task Force noted that the total future MilSatCom capacity for 2010 is anticipated to be below 4 Gbps. Most of this future capacity will be provided by the wideband Gapfiller, a unidirectional, unprotected broadcast system intended to support secondary dissemination of intelligence products and imagery. Advanced EHF will be the DoD "protected" system addressing unique military mission requirements. Although the Task Force recognizes that all telecommunication media need to be leveraged (as it is done today) to meet the ever growing DoD requirements, it is evident that the planned MilSatCom system architecture of the future will provide an order of magnitude less capacity than the conservative estimate for 2 MTW of 35 Gbps. It is important to note that the total capacity provided by UHF Follow-On (Mobile User Objective System beyond the Program Objective Memorandum) does not register on the scale of the information provided in Figure 31.

Findings: DoD – Requirements; DSB Assessment

- Projected *requirements* far *exceed current and planned* system *capacities**



* Extrapolated from the CMA study data for 2010

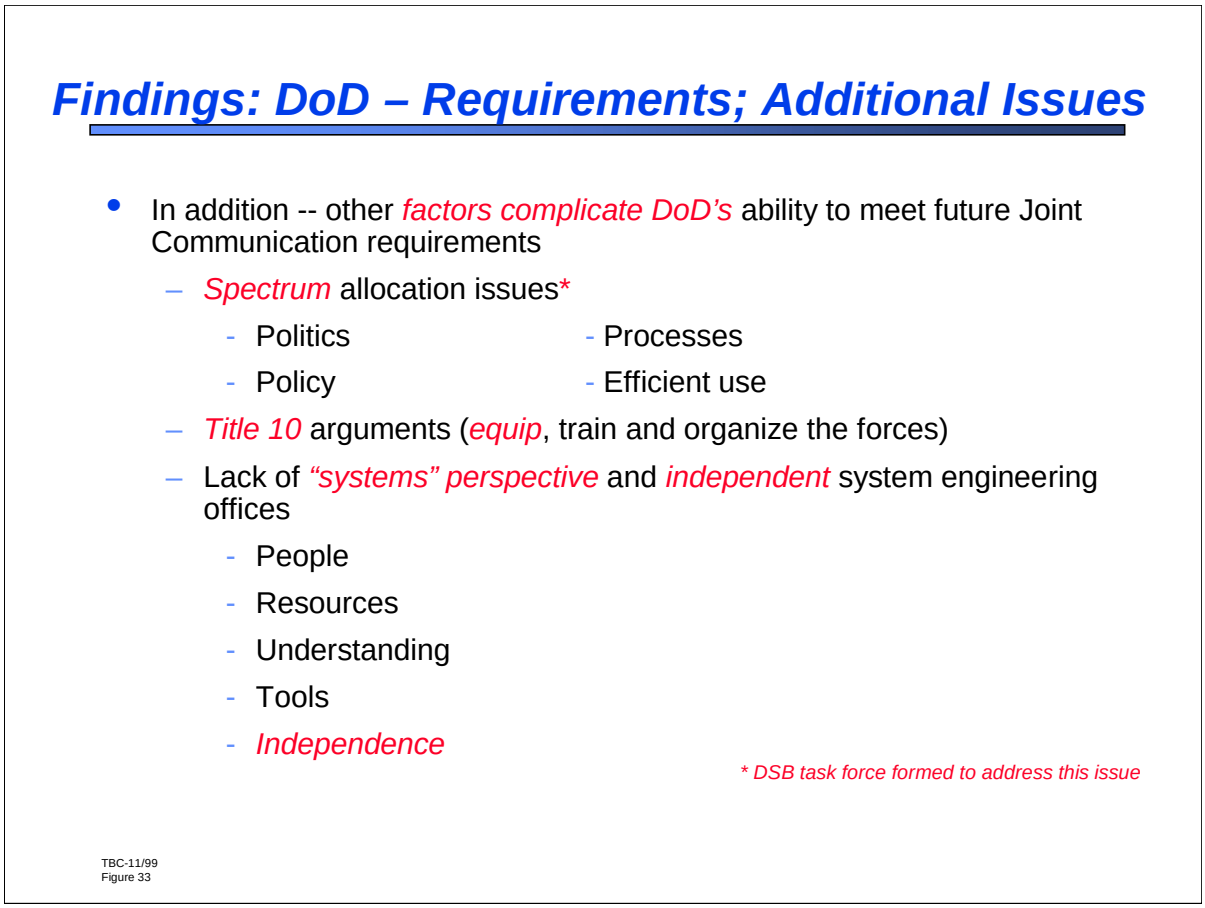
TBC-11/99
Figure 32

The Task Force also extrapolated to 2010 the result of the CMA study for aggregated bandwidths for information flow to deployed forces down to the Brigade level. The results of this extrapolation, shown in Figure 32, tend to show that existing communication systems and technology, especially for our ground force, will not meet the anticipated needs. Once again, the assumption underlying this extrapolation is that organic tactical ISR systems, focused logistics and warfighting concepts such as Joint Rapid Operations Forces (DSB), Joint Strike Force, and the like will all require greater communications capacity at the lower echelons of deployed forces.

Supporting this finding are experiences from Field Training Exercises (FTXs) and Advanced Warfighting Experiments (AWEs) which have shown that existing Service communication infrastructure, particularly for ground forces, are severely stressed as the forces become "digitized." Although work-arounds have been implemented for the near term, the situation will only get worse as more digitized systems are introduced into our forces C4ISR and weapon-system infrastructure.

In summary, the Task Force believes that DoD communications systems supporting the deployed warfighter currently can support only a small fraction of the projected future information transport requirements. These shortcomings are of particular concern when DoD is developing the future warfighting strategy envisioned by JV2010 that relies heavily on the timely

delivery of information to the forward deployed forces. The realization of JV2010 will undoubtedly involve broader dissemination of information as well as a dramatic increase in the use of real-time interactive technologies such as VTCs and collaborative planning. These requirements, as well as the emerging needs for supporting medical and logistics data, can only be realized if warfighter telecommunication resources are increased by at least two orders of magnitude in total integrated capacity over the next decade.



The need to provide additional telecommunications infrastructure to our CINCs and the forces they will fight is a difficult undertaking not only from an acquisition, fielding and ownership perspective, but also from numerous other factors as well. Figure 33 provides a list that highlights a few of these factors.

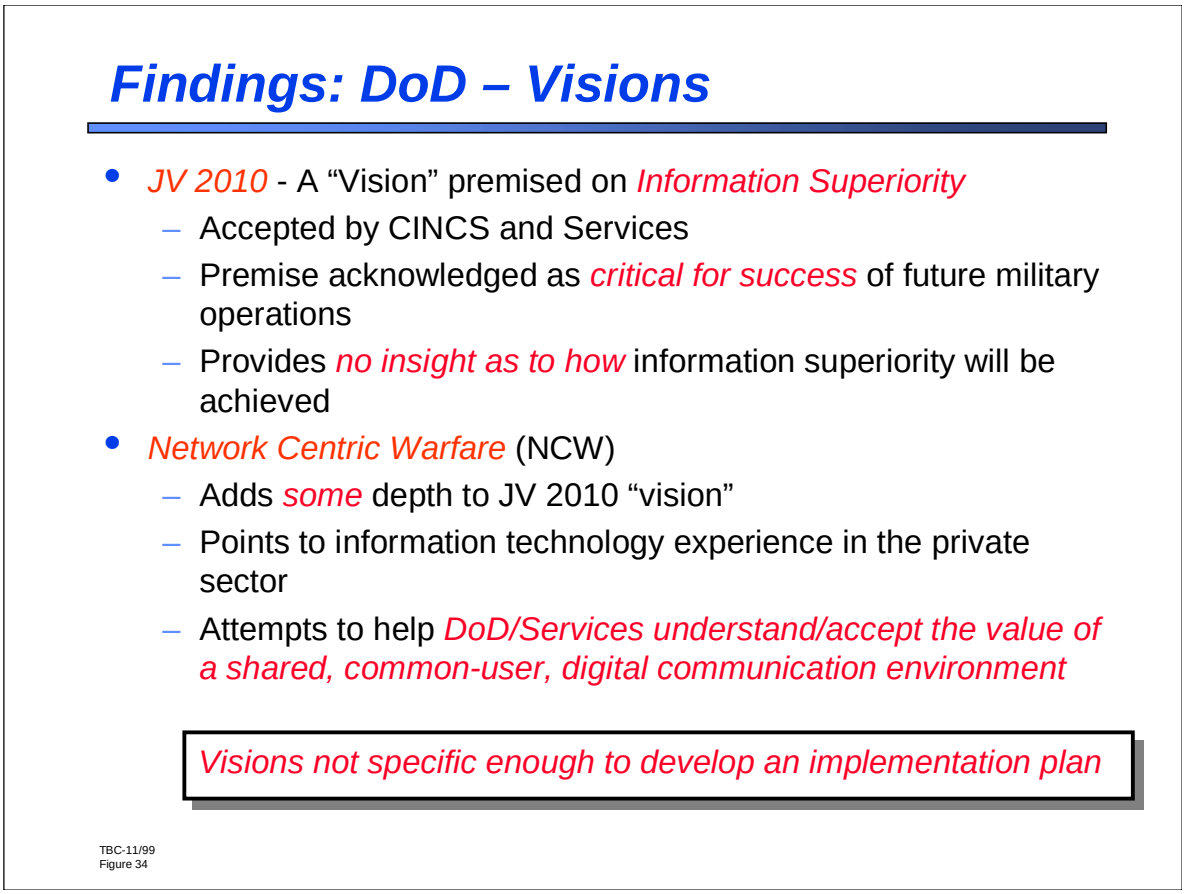
The Task Force received a briefing on issues associated with the use and retention of the radio frequency spectrum assigned for military use. The issues associated with spectrum assignment, its efficient use, and its effective management, are many and diverse and include the worldwide demand for spectrum by the private sector for wireless consumer telecommunication systems; the lack of a unified DoD policy and strategy on the spectrum needed for military operations worldwide; and the conflicting military needs for higher-capacity, antijam waveforms in its assigned fixed segments of the spectrum. It was also noted by the Task Force that although spectrum is addressed and managed as a stand-alone resource, in reality it must be viewed as an integral and essential element of the system design associated with an integrated DoD telecommunications infrastructure. OSD has requested that the DSB establish a study to address, in depth, the issues associated with Spectrum. That study is underway.

Another factor impacting the delivery of an integrated telecommunications system to support CINC warfighting needs is the Title 10 arguments made by the Services regarding their

responsibilities to equip the forces. Title 10 is often brought forth as authorization for the Services to pursue the acquisition and fielding of telecommunication systems that they feel meet their respective Service requirements. This strategy results in a system and technology "push" to the CINCs from the Services, as opposed to a requirements "pull" from a CINCs (customer's) perspective. The outcome of this Service-centric process results in the challenges in meeting the objectives of such programs as the JTRS (Annex D); duplicative acquisitions across the Services; and the interoperability difficulties experienced by the CINCs, as discussed earlier.

Finally, the Task Force noted that there is a lack of individuals with systems engineering skills and vision within OSD. In many of the briefings presented to the Task Force, excellent engineers presented the merits and technical details of the telecommunication system they were responsible for acquiring. However, no individuals could articulate how these systems would interoperate, what the architectural framework was that would facilitate this interoperability, or what the long-term vision is for a joint information infrastructure. The Task Force noted that the individuals who briefed were passionate about and dedicated to their mission. That mission was, however, in nearly all cases the mission of their parent organization, Service, or office. The Task Force observed that this passion limited an open, constructive debate between the briefers and the panel members regarding how a system would interoperate with others, whether other alternatives should be considered (such as a private-sector system), or even whether another Service's system and/or technology would meet the goals of the system being described.

The Task Force noted that an independent (not politically constrained) office of visionary system engineers, supported with adequate tools and facilities, could be an important resource to help DoD put in place an integrated, secure virtual Intranet to meet the future information and telecommunication requirements of our military.



Although the Task Force could not identify codified requirements for joint information exchange and a commensurate technical vision for a specific information infrastructure to support these requirements, the panel did find that DoD has established several visions for the future of military warfighting. Two examples of these visions are Joint Vision 2010 (JV2010) and Network Centric Warfare (NCW).

JV2010, as articulated by the Joint Chiefs of Staff, is: "the conceptual template for how we will channel the vitality of our people and leverage technological opportunities to achieve new levels of effectiveness in war fighting." It develops four overarching operational concepts that are enabled by improved intelligence and command and control, based on a capability delivered by the "information age." This new capability has been called *information superiority*. The CINCs and Services have accepted the vision and acknowledged it as critical to the success of future military operations. It is not intended as a prescription for how to create an environment of information superiority. Rather, as General Shalikashvili's introduction recognizes, it is an "operationally based template for the evolution of the Armed Forces."

The JCS-J6 NCW vision tries to add depth to the JV2010 and clarify the meaning of information superiority. One of NCW's primary themes is that a critical enabler for future combat effectiveness is a shared, common user, digital telecommunications environment. The basic idea has been captured in the private-sector Internet, or Metcalf's Law, which states that the value of an Internet grows with the square of the number of people and entities interconnected.

In other words the flattening of the information exchange hierarchy is fundamental to the process reengineering that is occurring in the private sector. However, while advocating the value of such fully integrated information infrastructure, NCW is not specific enough for the DoD and the Services use it to develop a consistent vision and implementation plan for such an infrastructure. In fact, nearly every briefing received by the Task Force on acquisition plans and strategy for military telecommunication systems has reverted to a circuit-centric view of dedicated communications stovepipes.

Findings: DoD – Information Infrastructure Concepts

- *Numerous* Information Infrastructure "concepts" for achieving information superiority are emerging from various communities
  - Examples
    - Global Information Grid (OSD/J6)
    - Global Grid (AF)
    - Global Grid (NRO)
    - Infosphere (AFSAB)
    - Integrated Information Infrastructure (DSB)
    - Living Tactical Internet (Army)
    - Naval Command Information Infrastructure (NSB)
    - Global Grid Architecture (FFRDC)
  - All are attempting to *add either process, policy, requirements or technical depth* (from a Service or OSD perspective) to JV 2010, and NCW

TBC-11/99
Figure 35

Despite the absence of a technically detailed DoD-wide vision deployment process and concomitant implementation plan for an integrated information infrastructure (GIG), numerous concepts for achieving information superiority are emerging from various DoD communities. These efforts have mostly fallen under the term "Global Grid." According to the Defense Technical Information Center, a Global Grid is an open systems architecture that provides global connectivity instantaneously on the warrior's demand. The global grid will support both vertical and horizontal information flow to joint and multinational forces. Examples briefed to the Task Force included the Global Information Grid (OSD/J6), Global Grid (NRO), Global Grid (AF), Living/Tactical Internet (Army), Naval Command Information Infrastructure (NSB), Infosphere (AFSAB), Integrated Information Infrastructure (DSB), and Global Grid Architecture (FFRDC). Each of these information infrastructure concepts is attempting to add process, policy, requirements, or technical depth (from a Service or OSD perspective) to JV2010 and NCW. Examples follow.

The Global Information Grid (OSD/J6) supports Network Centric Warfare by proposing a single secure grid that provides seamless end-to-end information services to all warfighters. These capabilities are to be provided by a joint, high capacity, bandwidth-on-demand network of networks fused with C4ISR systems and our military weapons systems. The intention is to achieve plug and play interoperability between users from the U.S., allies, and coalition partners.

Implicit in this concept is the inevitable blurring of the classical distinction between strategic, tactical, and base-post-camp-station communications. Essential to this concept is a strategy to defend the network in depth against all threats.

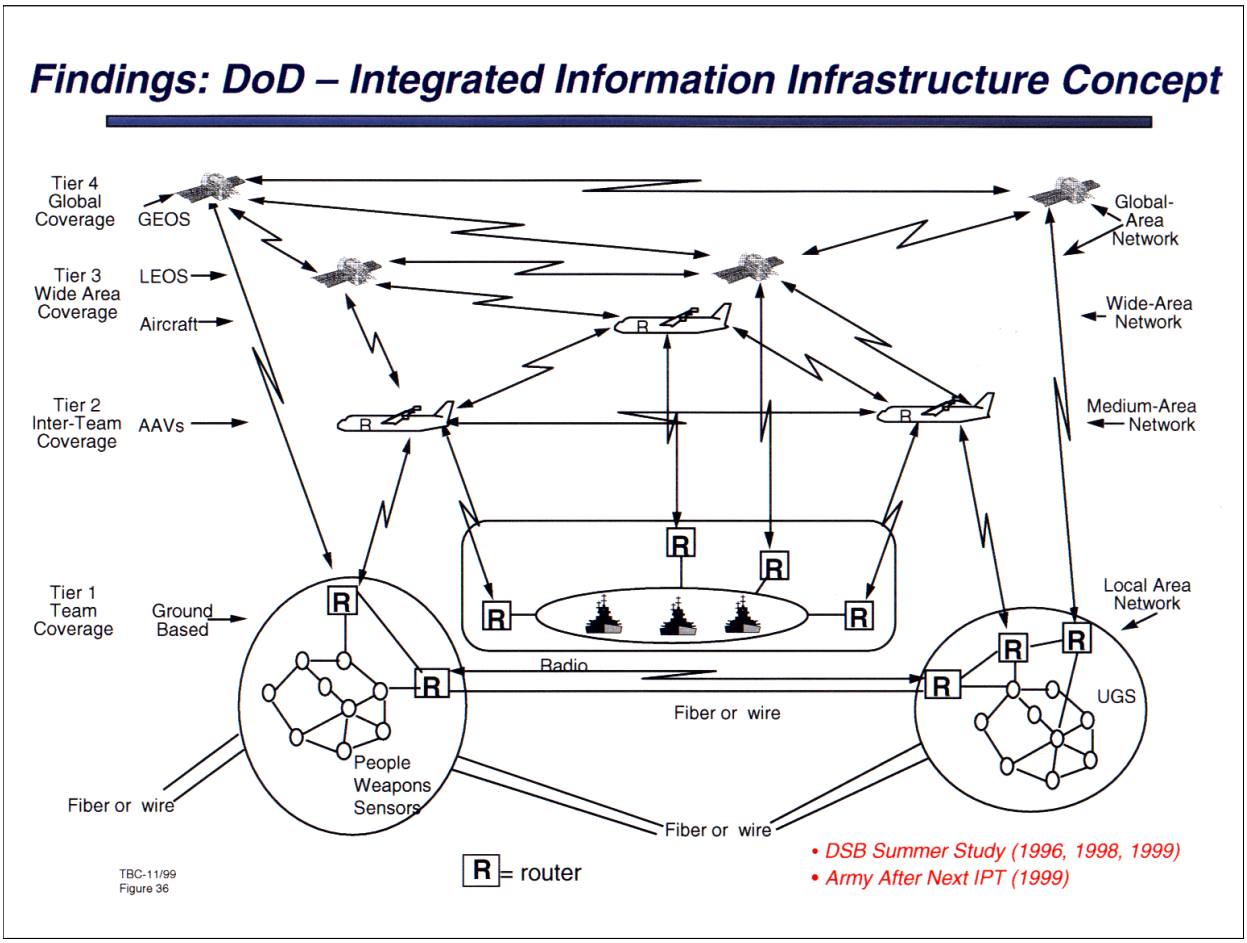
The concept has six components. Five are ordered hierarchically: Foundation, Communications, Computers, Global Applications, and Weapons. The sixth, Network Operations, extends across all components. In the area of the present study (telecommunications), the presentation identified key supporting initiatives: Backbone Network, Deployed/Shipboard Communications, base-post-station telecommunications, STEP Teleport, JTRS, MilSatCom, Advanced EHF, Coalition Wide Area Network (CWAN), and Last Tactical Mile. However there was no identified means of synergistically managing these series of investments.

The Global Grid National Reconnaissance Office (NRO) is a concept and experiment intended to achieve an infrastructure to support NRO product dissemination; it was initiated in response to lessons learned in Desert Storm. The concept and experiment are addressing the development of a secure, interoperable, and scaleable information infrastructure that is commercially derived and DoD controlled. The Global Grid has focused on the integration of a high-capacity, native ATM-based backbone network that supports interactions between CINCs and major intelligence facilities. In parallel, it has also focused on the broadcast-based dissemination of intelligence products and has supported initiatives to improve the interoperability between tactical telecommunication networks. It provides ATM services to the end-user device.

Global Grid (AF) is an Air Force initiative to provide the communications utility for the information appliances that will support future Air Force missions. The Air Force is using this activity to harmonize its communications efforts, both within the Air Force and with the larger DoD community. At the service level there is an emphasis on finding ways to provide communications modernization within the constraints imposed by the platform acquisition process. This work is supported by FFRDC efforts to extend the global grid to the airborne domain.

The Tactical Internet (Army) effort was begun in support of the Army Digitization Vision. Its first focus has been on integrating legacy tactical communications into an internetwork. This effort has been generalized in the Warfighter Information Network.

The Defense and Service Science Boards have all articulated concepts for their particular domains. The Army Science Board participated in the evolution of the Army After Next (AAN) concept; the Naval Studies Board (NSB) has developed the Naval Command Information Infrastructure concept; the Air Force Science Advisory Board (AFSAB) has developed the Infosphere concept; and the Defense Science Board has developed the concept of a DoD-wide Integrated Information Infrastructure (III) or, equivalently, a Global Information Grid.



The III was first advocated in the 1996 DSB summer study* and updated each subsequent year. It was endorsed by the Army in 1999. This concept showed how to integrate different scales of operations (local, medium, wide, global areas) taking place across land, sea, and air. It advocates the use of commercial, standards and technology to integrate the different transmission media (wire, fiber-optic, SatCom) into a coherent information-bearing infrastructure on top of which an interoperable intelligence and C2 infrastructure can be built.

The transport layer of the III consists of four tiers, as shown in Figure 36. These tiers are conceptual, because the interfaces between them are seamless and transparent to the user—tiering serves only to relate the information infrastructure to organizational and doctrinal concepts. In fact, any entity in the information infrastructure can automatically and directly exchange information (and interact with any other entity). While we expect that such ubiquitous connectivity will be a very powerful force multiplier, we also expect traditional organizational

*"Tactics and Technology for 21st Century Military Superiority," October 1996; "DoD" Responses to Transnational Threats," December 1997; "Joint Operations Superiority in the 21st Century," October 1998; "Defense Technology Strategies for the 21st Century," October 1999.

and doctrinal constructs to change more slowly than the technology that makes such connectivity possible.

The first tier of the transport layer is the tactical component. This infrastructure component comprises local-area networks that provide voice and data services to entities operating together in integrated or support missions. These transport networks are store-and-forward, packet-switched systems that are self-managed and adaptive, and provide peer-to-peer data relay and processing. The networks adapt to changes in the locations (i.e., the mobility) of its end users; they have no centralized nodes or base stations that would enforce the use of a vulnerable star topology; and they automatically route information among participating nodes, based on real-time assessments of the network connectivity. These local-area transport networks can support a single person or a force structure of any size (through appropriate subnetting).

Although a few modest examples of peer-to-peer, wireless, packet-data communication systems are deployed in the private sector, the fundamental work in this type of technology has been and continues to be funded by the DoD. This trend will likely continue, given that the private sector's present view of ground-based wireless data communications is predicated on the notion of a deployed fixed infrastructure (base stations connected to the wire plant) to which, and through which, each mobile subscriber establishes a communication circuit. This commercial wireless system architecture is based on many years of legacy, circuit-switched, voice-based telephony systems. It also facilitates billing and related revenue-generating processes for mobile subscribers.

In contrast, the military has relied primarily on push-to-talk, broadcast, wireless communication systems for its mobile users. This system architecture, however, severely limits support for highly mobile users; for dynamic, flexible force structures; and for mission and time varying information transport requirements.

For these reasons, DARPA initiated a packet radio program in the 1970s. This technology-based program was intended to explore the notion of building intelligent radios that would be networked to provide the highly mobile warfighter with data services while on the move. These radios would self-organize into networks, automatically route (relay) information from any source to any destination within the radio network (or across the internetwork to other users), automatically adapt to failed nodes or stress exposed on the network by an adversary, and perform other similar network services. This technology base has resulted in systems such as the Army's Surrogate Digital Radio and the Near-Term Digital Radio. However, these systems will not fulfill the vision set for Tier 1 of the III. It is the research and development being pursued in the DARPA Small Unit Operations (SUO) and GloMo programs, if appropriately focused and guided, that will lead toward technology that will meet the Joint mobile warfighter needs. These programs will provide the fundamental knowledge and technology that will meet the network requirements set forth in the JTRS Operational Requirements Document.

It is anticipated that as these DoD-supported, technology-based programs generate stable technology (specifically, network algorithms and software), these technologies will ultimately be embraced in the private sector as the need for supporting data and voice services to mobile commercial subscribers manifests itself. This technology transfer to the private sector is, however, not anticipated to occur for many years, and will be driven by consumer demand for

such flexible, reliable, mobile data services and by the ascendancy to leadership positions in the telecommunications industry of individuals who relate to internetwork-based mobile data services.

At the second tier, the transport layer incorporates airborne networks and processors for data transport and information services among force entities that require connectivity beyond that supported by their local area network. To support this broader area coverage, we envision a swarm of Autonomous Air Vehicles (AAVs) that supports medium-area networking services. These platforms are cross-linked between themselves and other airborne and space-borne networks, as required, and are linked to the local-area networks (LANs).

The private sector is pursuing similar concepts of airborne-relay telecommunication platforms. Two such activities, which are currently raising capital, are the Skystation and Air Relay. The Skystation is conceived to be a station-keeping, lighter-than-air platform located 22 km above the earth. This proposed activity would provide 10 Mbps data services to every home within the service area covered by each platform. The Air Relay, will consist of aircraft-based telecommunication relays that will provide similar data services to ground-based users.

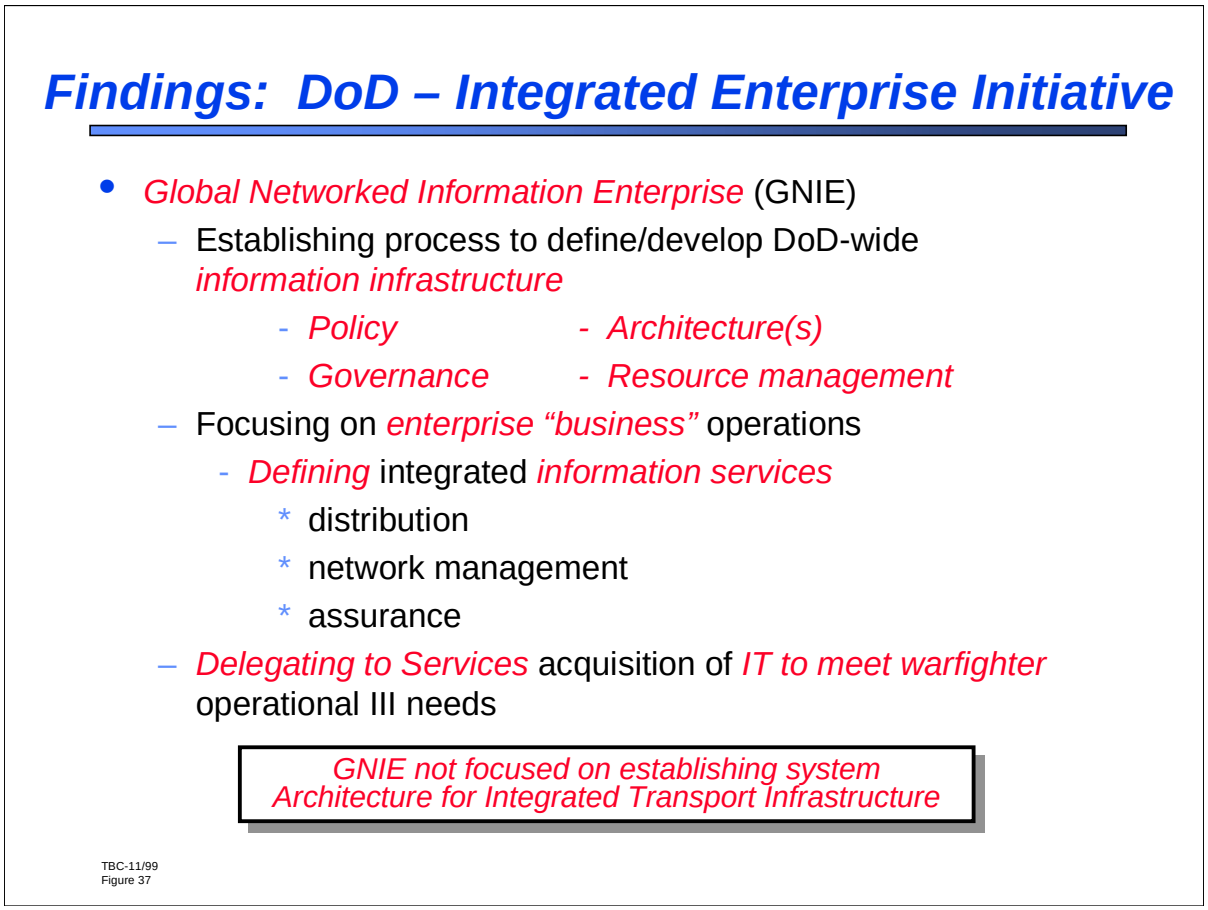
In both of these and similar commercial concepts, however, the system architecture (the location of platforms, relaying and switching, and bandwidth allocation) consists of parameters that are predefined and managed through centralized facilities. The military, however, needs much greater flexibility, adaptability, and autonomy for Tier 2 if the warfighting requirements noted above are to be met. Thus, in our vision of the III, the airborne platforms carry intelligent radio nodes that perform all of the functions and services of the Tier 1 LAN: automatic, adaptive packet-data routing and switching. All airborne nodes automatically integrate themselves into an airborne network, and the unmanned aerial vehicle (UAV) platforms automatically position themselves to provide survivable, fail-safe coverage of the ground-based units. Other airborne elements, such as mission aircraft, automatically provide relays of opportunity within the Tier 2 segment. The DARPA Airborne Communication Node (ACN) program is beginning to address this extended set of network services for Tier 2 of the III.

As noted in Figure 36, the airborne nodes are cross-linked not only to themselves and the ground LANs but also to the space segment of the transport element of the III. The airborne nodes act as pseudolites and carry payloads that are integrated into the various commercial satellite telecommunication systems that have been and will be deployed in the next 10 years. As an example, preliminary analysis indicates that a Teledesic package (700 kg) could be accommodated on a DoD High-Altitude, Long-Enduring (HALE) platform. With an appropriate antenna, an active phased array on the UAV, the pseudolite could provide high-bandwidth communications services to and between ground elements and could route traffic automatically to the commercial space segment for long-haul services. Other approaches can also be envisioned: for example, the pseudolite could use commercial satellites as trunk facilities between the airborne relays. The critical technical issues in realizing this richly interconnected, survivable airborne transport segment of the III are associated with the development of protocols and algorithms to provide adaptive network services.

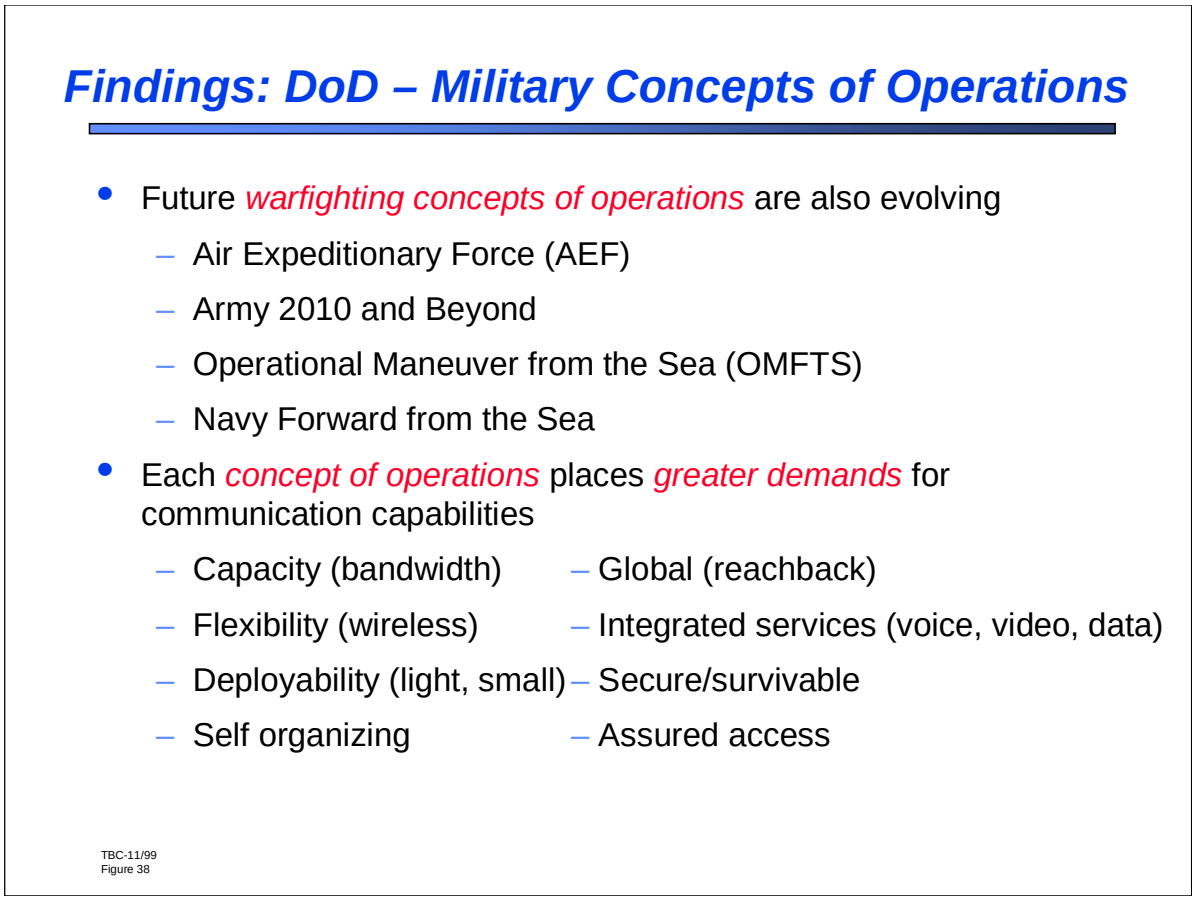
At the third tier, the information transport infrastructure provides connectivity over widely dispersed areas through the incorporation of LEO satellites. The fourth tier includes MEO and

GEO satellites for global coverage. The space-based transport segment of the III should be based primarily on emerging commercial technologies. At the present time, many such systems with widely varying characteristics are expected to be available by 2005, as discussed earlier in this report.

The routers, labeled "R" in Figure 36, are commercial Internet devices that maintain, in real time, knowledge about the entire transport layer's topology and connectivity. In conjunction with the intelligent software agents, the routers make dynamic decisions, based on this understanding, to ensure that information is transported from all sources to all destinations, as required. The richly interconnected tiers and the diversity of systems integrated by the routers provide a high degree of survivability for the transport layer of the III. Instead of providing jamming protection for the links of a specific system, the concept of multiple paths from any source(s) to any destination(s) forces an adversary to attack all of the integrated systems simultaneously. Given the diversity of operating parameters, the geospatial location of these systems, and the systems' footprint on the ground, such an attack would be exceedingly difficult to mount and then to sustain.



In addition to the many concepts that are emerging for a DoD-wide virtual Intranet, one program was attempting to cause such an infrastructure to come into being. The Global Networked Information Enterprise (GNIE), summarized in Figure 37, was an initiative established at the direction of the Deputy Secretary of Defense, and intended to deliver "secure, assured efficient, effective, interoperable information services, responsive, on a global basis—enabling successful warfighting, warfighting support, and business operations that provide National Security." GNIE was a response to the Clinger–Cohen Act of 1996 that mandated the executive agency to "develop, maintain, and facilitate the implementation of a sound and integrated information technology architecture." The objective of GNIE was to establish a policy, governance, architecture and resource management policies. As the program moved forward it focused on defining the integrated information services needed across DoD, with particular emphasis on improving the business operations. It delegated "tactical" information transport to the services. However, the warfighting concepts of operations demand a strategy for *integrated* information transport that moves information seamlessly between services at all levels. This failure to establish and enforce an integrated system architecture leaves the full realization of the JV2010 vision to chance, and subject to individual Service priorities.



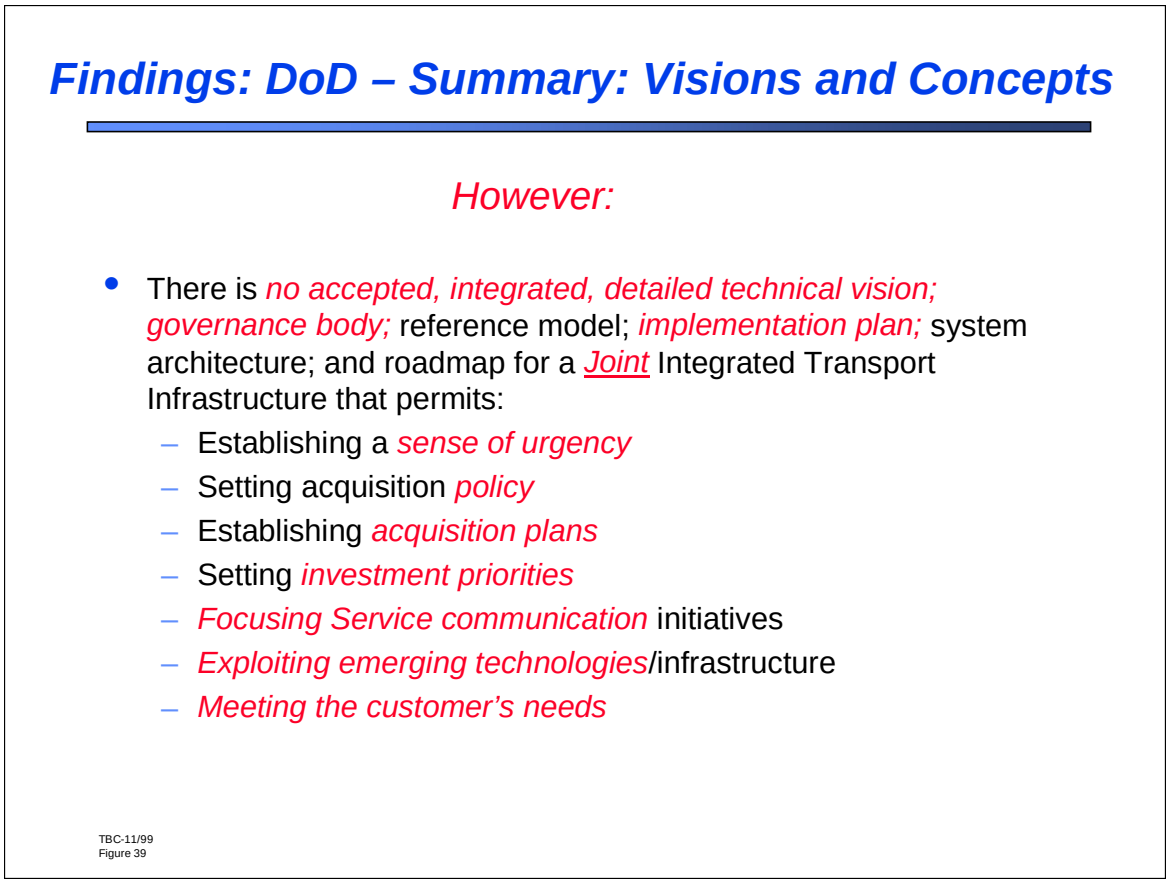
In addition to the visions and concepts being developed by the JCS, OSD and the many other DoD-related organizations discussed above, the Services are aggressively developing military concepts of operations for the future. Each of these concepts is a response to the changing post-cold-war threat environment that our nation faces. Issues such as the asymmetric threat, the lack of a near-term peer competitor, and the need to support early-entry missions have caused a reassessment of Service missions, roles, force structures, and force composition for the future. Although this reassessment is still underway, each Service has put forth preliminary concepts that include the following.

Air Expeditionary Force: (AEF) is an effort to achieve a rapidly deployable tailored force. The core strategy is to place combat power forward with a reachback to the rear for support. A wideband internetted telecommunication capability is fundamental to support such reachback.

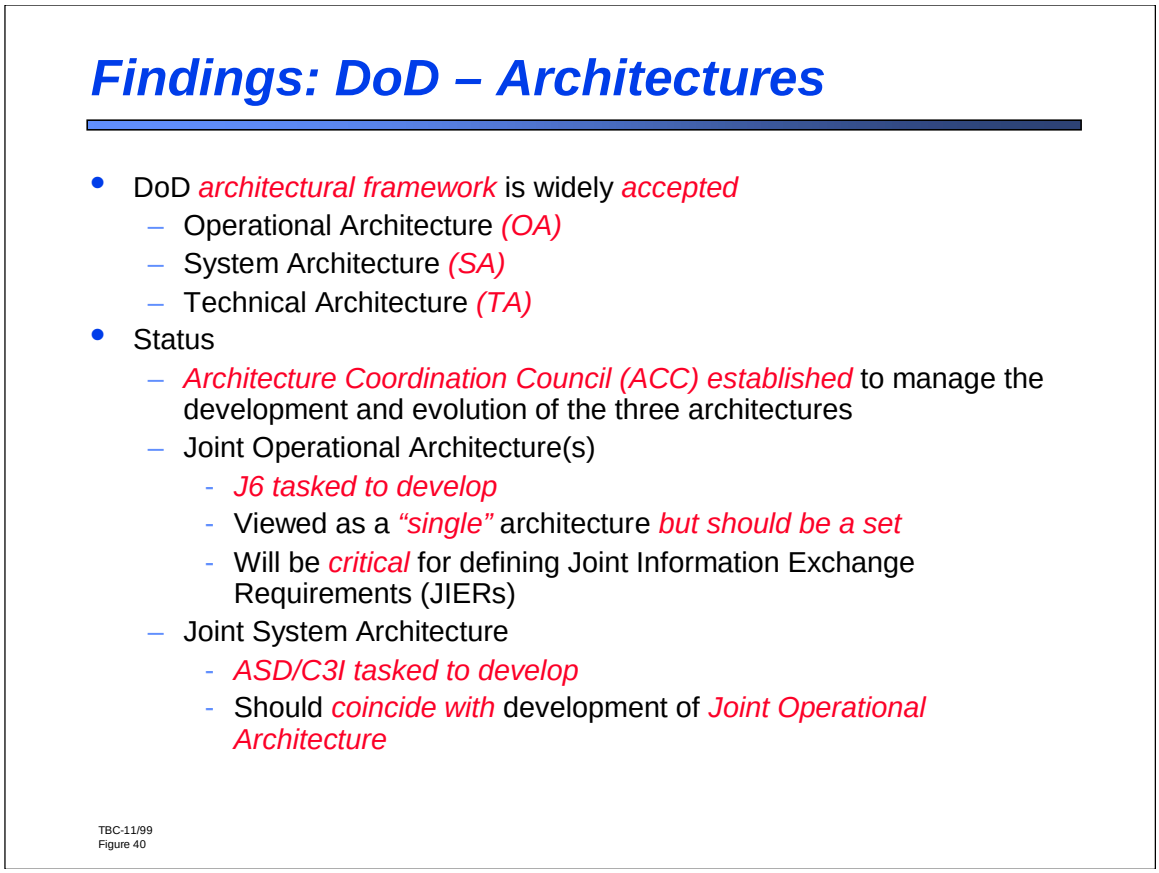
Army 2010 and Beyond: is a Training and Doctrine Command Initiative to conduct studies of warfare to about the year 2025. Its objectives are to frame issues in the development of the U.S. Army after about 2010 and to focus future combat development programs on these. One of the key transitions seen in the Army 2010 and Beyond initiative is the move from mental agility to physical agility of the force. Separate CECOM sponsored work on the communications support has emphasized an extensive utilization of space-based communications and identified a number of unique military needs that may not be supported by the commercial market place.

Operational Maneuver from the Sea: (OMFTS) is a concept that emphasizes the ability to perform flexible deep strike from the sea. It was emphasized to the panel that this concept requires over-the-horizon, highly integrated telecommunication. A number of Extended Littoral Battlespace (ELB) experiments have been undertaken to gain experience with potential approaches for meeting this requirement.

It is interesting to note that each of these concepts of operations imposes increased demands for a flexible, scalable, integrated military communications infrastructure. In several cases, the evolving concepts require greater capacity from the underlying telecommunication infrastructure as well as new or expanded information services. These demands cannot be satisfied with the present and future military communication systems DoD is planning to procure.



DoD visions, evolving concepts of operations, and evolving CINC/Service communication requirements all point towards the need for an integrated, joint, DoD-wide virtual Intranet with an aggregated telecommunication capacity much greater than that which exists or is likely to be put in place within the next decade. Thus, despite the premise of information superiority that underlies the "revolution in military affairs," the Task Force feels that the probability of realizing the premise or visions is low. Without a *detailed* technical vision, governance body, reference model, implementation plan, system architecture and road map for a joint integrated transport infrastructure, little progress will be made toward achieving the GIG. Such is needed to set acquisition policy, establish acquisition plans, set investment priorities, focus Service telecommunication acquisition initiatives, exploit emerging technologies/infrastructure and, in the end, meet the users' needs. It should be noted that a detailed technical vision is called for within DoD. In contrast to the simple, high-level vision for the Intranet that exists in the private sector, a vision that is realized through customer demand and market forces, a detailed vision is needed in DoD to help focus and direct the many telecommunication acquisition programs toward a common goal.

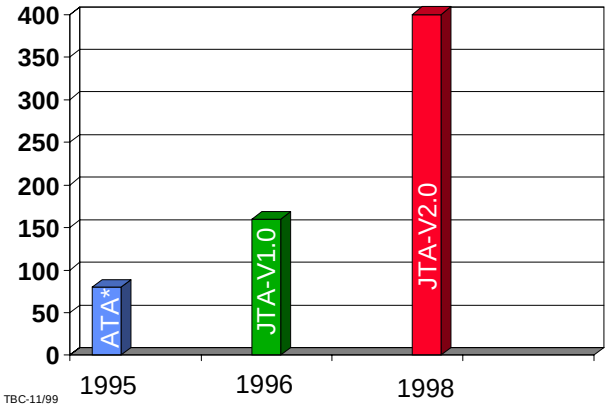


If DoD decides to implement an Intranet, it does have tools in place. Specifically, the DoD architectural framework, comprising the Joint Operational Architecture (JOA), the Joint Systems Architecture (JSA), and the Joint Technical Architecture (JTA), is widely understood and reasonably well accepted by the Services. An Architecture Coordination Council (ACC) has been established to manage the development and evolution of the three architectures. The J6 has been tasked to develop the JOA, which is viewed as a single architecture but should be viewed as a set representing a mix of JTF force structures and corresponding missions. This set of OAs will be critical for defining JIERs.

The ASD/C3I has been tasked to develop the JSA, which can be developed concurrently with the JOA. The JSA could be used to define how various telecommunication systems would be integrated into a DoD-wide virtual Intranet.

Findings: DoD – Architectures

- Joint Technical Architecture
  - Goal: Insure and facilitate C4ISR system *interoperability*
  - *Standards-based –* DoD and commercial
    - * *Includes IP* and *related* commercial *standards*
  - *Hindered by consensus-based management philosophy*
    - * Number of *standards growing* with time



TBC-11/99
Figure 41

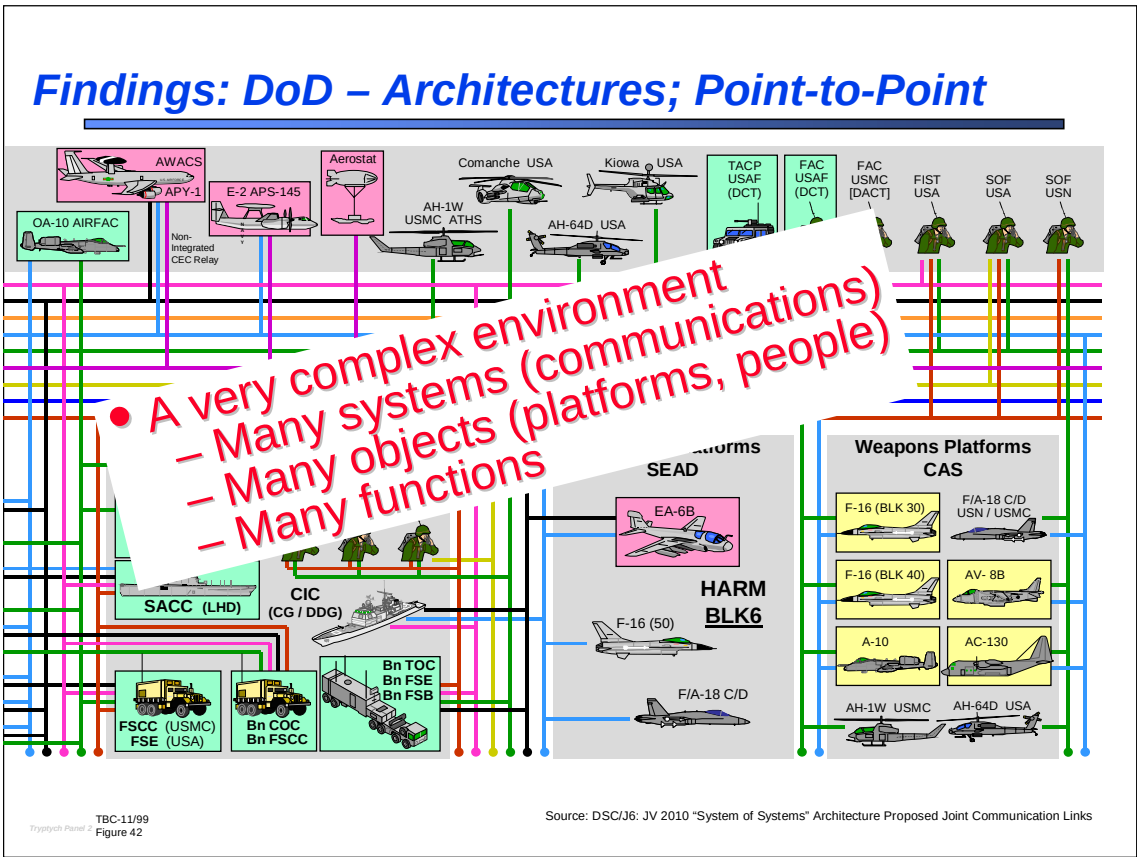
Growing number of overlapping standards for similar information services defeats the JTA goal of facilitating C4ISR interoperability

*ATA – Army Technical Architecture

The JTA, in turn, could be the standards foundation upon which the DoD-wide virtual Intranet could be built. The present goal of the JTA is to facilitate C4ISR system interoperability from the transport (telecommunications) level to the application level of these systems. As originally conceived, it was to be a minimal set of protocols and standards, primarily drawn from the private sector, that would enable the integration and interoperability of acquired or developed DoD C4ISR systems within an Internet-type framework. In fact, the JTA does comprise many of the essential standards that underlie the private-sector Internet, to including IP and related standards.

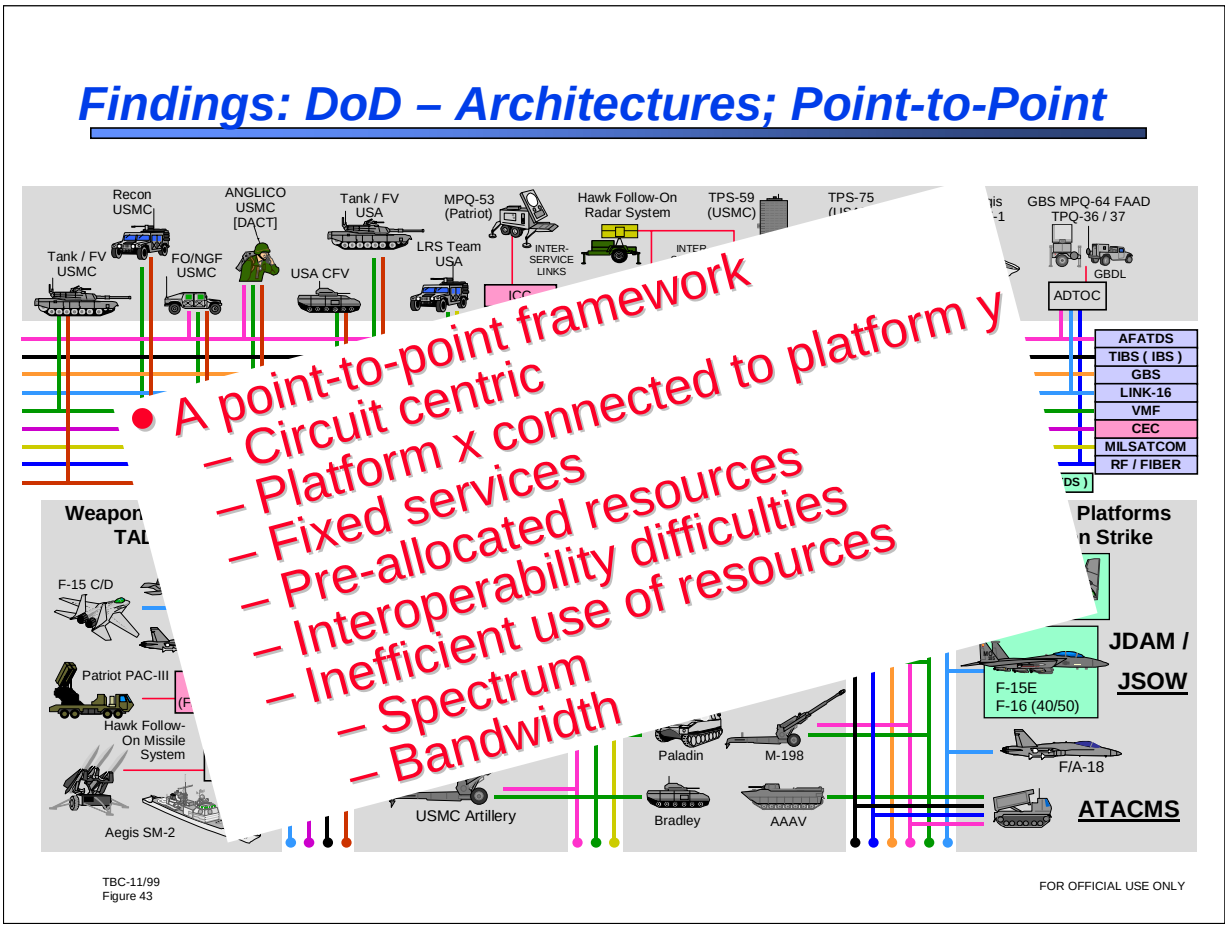
However, the Task Force noted that the number of standards in the JTA has grown with time, partly due to the development of new standards for the Internet, partly because the JTA covers new DoD functional domains and partly because the Services want the JTA to include standards for their legacy systems.

Task Force discussions with present and past Service personnel who participate in the JTA standards update processes, indicate that the consensus-based process of introducing standards tends to minimize dissention by including military and other standards when a strong lobby is presented. This approach to managing the JTA has the potential disadvantage of turning the JTA into an architecture with multiple standards supporting the same information service. This overlap would result in defeating the original interoperability goals set for the JTA.



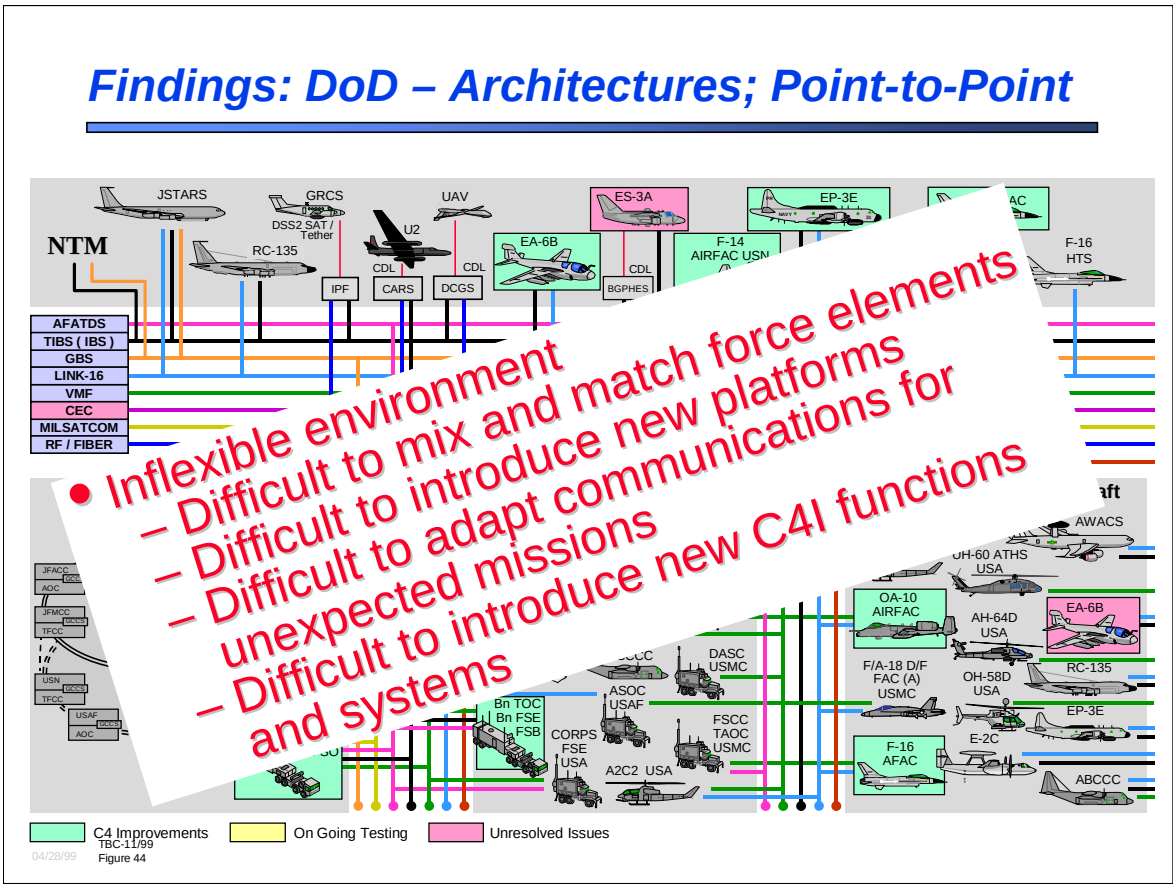
Included in the JTA are numerous military standards for communication services. These standards, and the systems that are presently fielded by the Services that embody these standards, primarily support circuit-switched based, point-to-point (or broadcast) connections. The Task Force noted that this system architecture is the same construct that had existed in the private-sector telecommunications infrastructure; however, the private sector is rapidly converging to a common-user, dynamically shared, QoS-based architecture. The value derived from this transition in the private sector is as discussed earlier, the ability to dynamically share information between any number of users on the Internet as well as the more efficient use of telecommunications resources through the dynamic, real-time allocation of Internet capacity and processing resources.

The current DoD C4ISR systems clearly represent a very complex environment consisting of many communication systems, objects (platform, people), and functions, all designed to meet very specific requirements. As shown in Figures 42–44, these entities (systems, people, and platforms) exchange information through point-to-point connectivity, fixed services, and preallocated resources, resulting in the inefficient use of bandwidth and radio-frequency spectrum.



These inefficiencies result from the preallocation of resources—fixed frequencies assigned to radio systems, capacity on circuits assigned to specific warfighting functions (intelligence, logistics, C2, and the like) and telecommunication systems assigned to specific platforms irrespective of the usage of these resources. Thus, requests for a dedicated T1 (1.544 Mbps) circuits (capacity) might be made by a functional proponent, even though the circuits might not be used continuously at full capacity.

Furthermore, interoperability issues are introduced by DoD's system design methodologies. To get information to transit from a Joint Tactical Information Distribution System (JTIDS) to another radio-based network requires that the tactical digital information link, type J (TADIL J) message be decoded at the application level and reformatted into an appropriate message structure for transport across the other network. These types of interoperability issues arise because DoD has, in many instances, tightly coupled the message syntax (format) to the channel characteristics of the supporting telecommunication system—the latter thus becoming an application-level device. In contracts, the Internet telecommunication fabric transport bits—the meaning of which is transparent to the telecommunication switches, radio components and the like. Thus, bits can easily flow across network boundaries (in this network of networks) in order to move information from any source(s) to any destination(s). The only syntactic (structure) information understood and used by the telecommunications infrastructure is source and destination addressing, and QoS specifications in the packet of bits being transported.



Another limiting factor inherent in DoD's telecommunications infrastructure is its inflexibility. Because of the circuit-based, point-to-point (and broadcast) framework embedded in numerous radio systems, if a platform must communicate with an unanticipated entity (for example, Air Force bombers communicating to Army ground forces, or a mechanized company communicating with its senior command), additional radios must be incorporated into one or both platforms to provide the circuit. As a result, many operational facilities (OPFACs) must have numerous radios, resulting in information interoperability problems, radio frequency interference, and platform real estate problems.

This situation should be contrasted with the rapidly converging Internet and PCS system architectures. Typically, a user of the Internet has one wired means of access into the Internet, over which all information services are provided. Similarly, PCS phones are becoming multiband and multimode, thus providing one wireless interface for a user to obtain both data and voice services while on the move anywhere in the world. This flexibility in access to and movement of information across the Internet is its inherent power. People (entities) come together dynamically to conduct business, solve problems and exchange information to meet their needs whenever and wherever necessary. When transactions are completed, Internet resources are made available for others to use—the value of the Internet is its providing connectivity to all from all when and where needed.

Findings: DoD – Architectures; Internetworked Systems

- *Combat effectiveness enhanced through Internetworked systems*
  - *Ground Operations examples*
    - Based on Modeling and Simulation results

	Before	After
Plan Development (Division)	72 Hours to Complete	12 Hours to Complete
Call for Fire	*3 Minutes to Complete*	*0.5 Minute to Complete*
Deliberate Company Attack	*40 Minutes* to Initiate	*20 Minutes* to Initiate
* Hasty Company Attack	*LER** = .49*	*LER = 1.24*
* Defense in Sector	Red penetrates Blue defense *LER = 1.01*	Blue stops Red penetration *LER = 2.45*
* Movement to Contact	*LER = 1.10*	*LER = 1.65*

Internetworking made the difference between FAILURE and SUCCESS!

* Task Force XXI Army Warfighting Experiment Integrated Report: Modeling of Opportunities

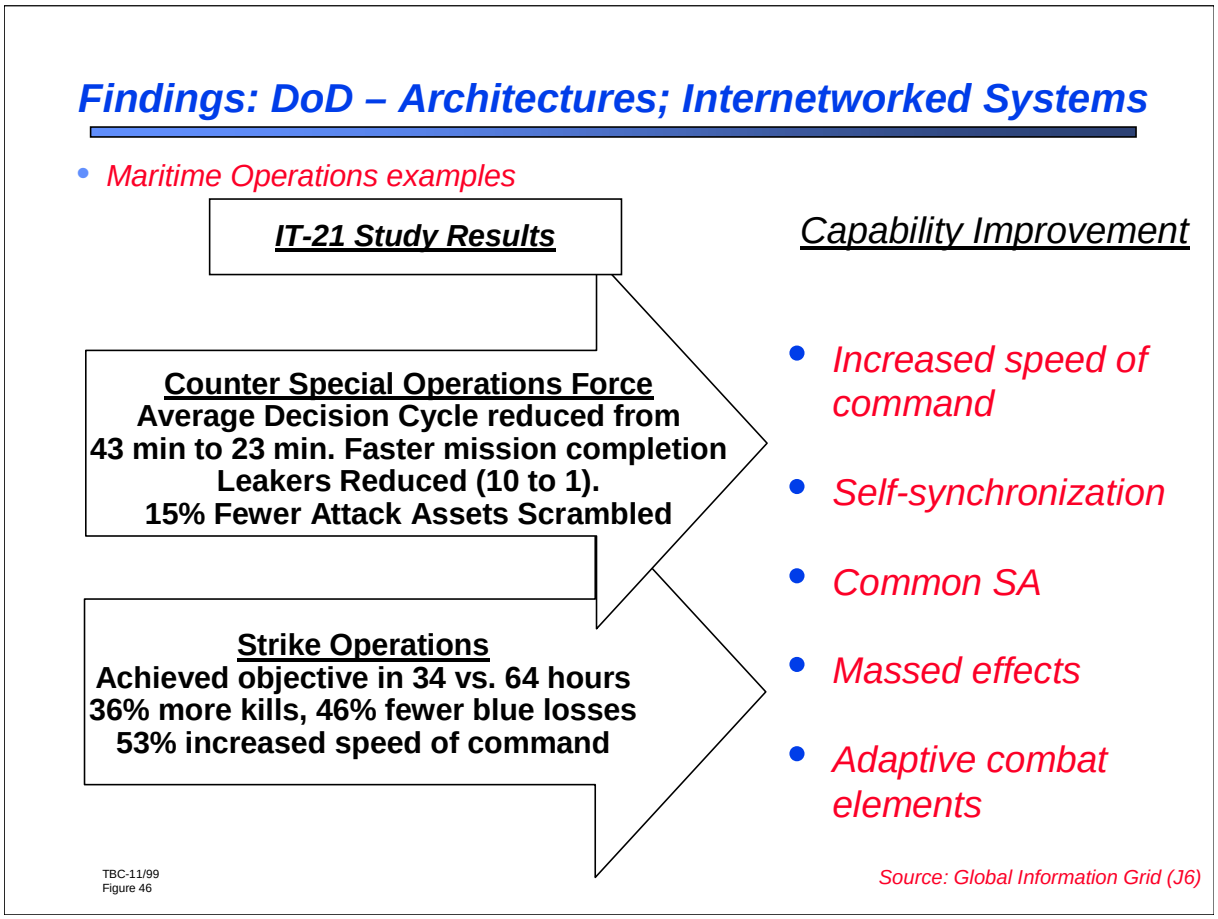
** LER = Loss Exchange Ratio = # of Red Losses/ # of Blue Losses (Bigger is Better)

TBC-11/99
Figure 45

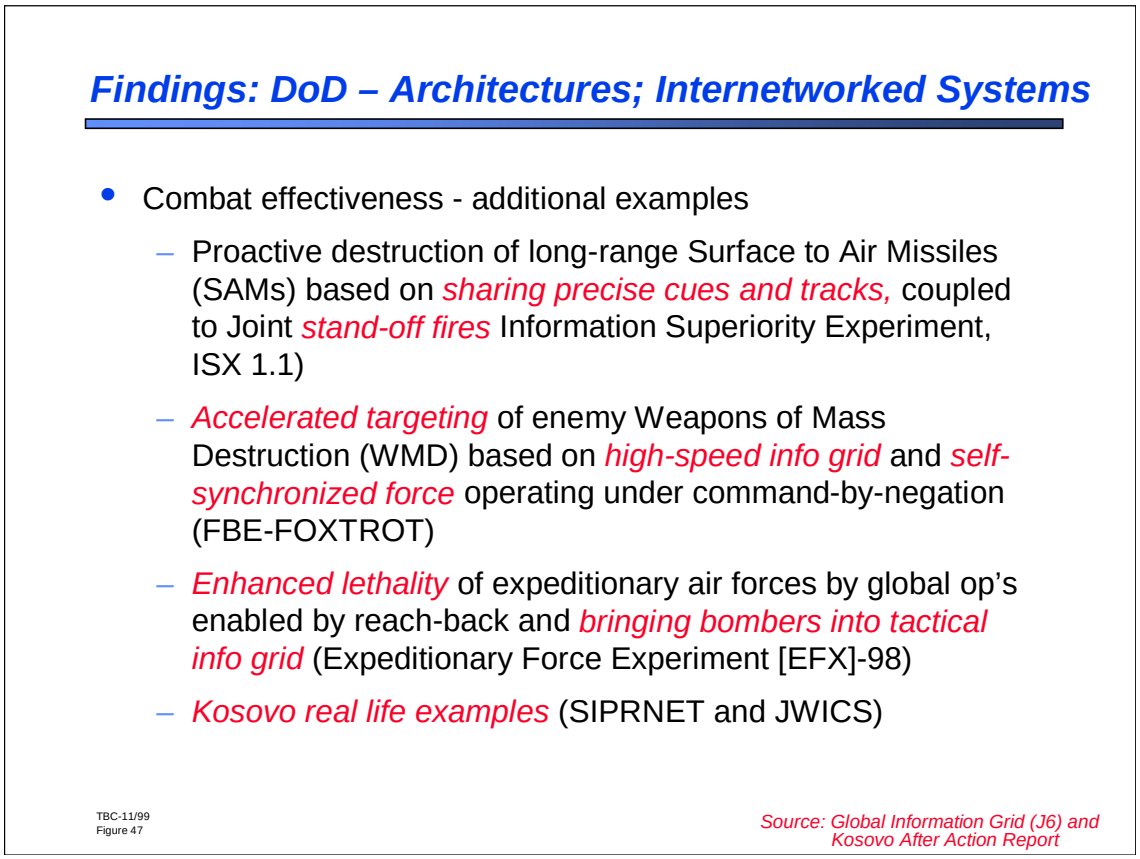
Source: Global Information Grid (J6)

The value of internetworking telecommunications within DoD to increase combat effectiveness has been shown in various modeling and simulation efforts (referenced in the GIG study conducted for the J6). These efforts have shown that internetworking will allow commanders and warfighters to use information effectively to organize, deploy, employ, and sustain their forces according to the needs of the mission. Internetworking would increase combat effectiveness, resulting in higher lethality and lower casualties, higher likelihood of closing kill cycle on mobile targets, greater responsiveness and agility, increased deployed firepower on demand, and reduced logistics timelines.

For example, the Task Force XXI Army Warfighter Experiment Integrated Report captures simulation results that show how internetworking can make the difference between the failure and success of a military operation. Specifically, the results indicate a significant increase in the loss exchange Ratio (number of Red losses/number of Blue losses) as a result of internetworking (shown in Figure 45).

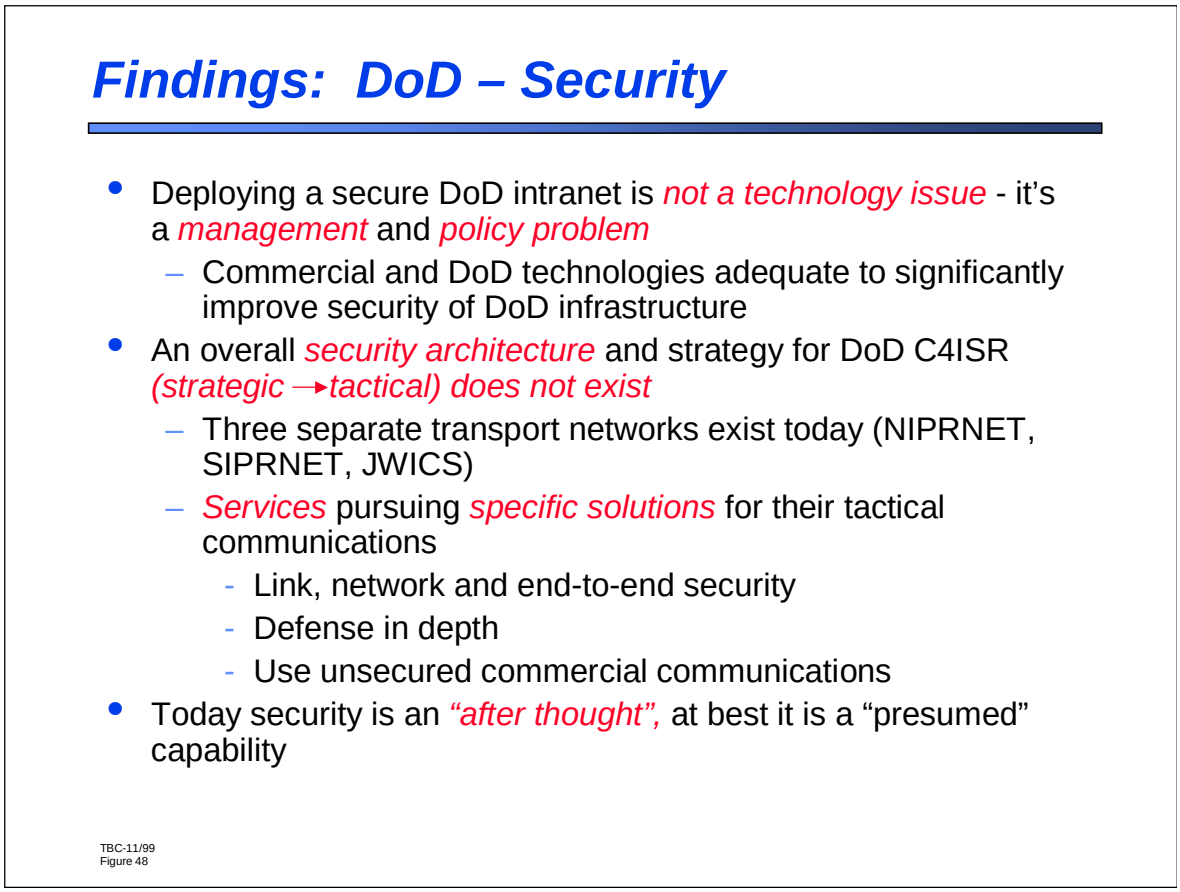


Similar results have also been observed in maritime operations; e.g., the IT-21 study results for Counter Special Operations Forces and Strike Operations showed that internetworking resulted in improvements in military combat effectiveness, due to the increased speed of command, self-synchronization, common situational awareness, and the ability to mass effects, as indicated in Figure 46.



Additional examples highlighting the value of internetworking for increasing combat effectiveness include several field experiments and real-life operations (see Figure 47). During the Information Superiority Experiment (ISX) 1.1, it was shown that sharing the precise cues and tracks of long-range surface to air missiles (SAMs), coupled to joint standoff fires, resulted in proactive destruction of those targets. In FBE-FOXTROT, the use of a high-speed information grid and self-synchronized forces operating under command by negation resulted in accelerated targeting of the enemy's weapons of mass destruction (WMD). Similarly, in Expeditionary Force Experiment (EFX)–98, it was shown that the lethality of expeditionary air forces could be enhanced by the use of an information grid that provided global reach-back and integration of the bombers into a tactical information grid.

Finally, the operation in Kosovo was a real life example of increased combat effectiveness achieved by using the SIPRNET and Joint Worldwide Intelligence Communications System (JWICS) as Internets supporting real-time intelligence dissemination and multiparty video teleconferencing (VTC). The latter service is reported to have significantly reduced the time necessary for command decision-making and promulgation.



If the DoD were to deploy a DoD-wide virtual Intranet, the question arises as to whether it can be made secure. This question was asked of the Task Force several times, the issue being the perceived vulnerability of the Internet in the private sector. As noted earlier in this report, the Intranet—originally conceived and designed to provide easy and open access to any information on the Internet by all users—is rapidly developing technology to secure information transactions and to protect the infrastructure.

In fact, the U.S. House of Representatives is pushing HR 2413 which has at its core two goals: assisting the National Institute of Standards and Technology (NIST) in meeting ever-increasing information security needs within the federal sector; and to allow the federal sector, through NIST, to harness the ingenuity of the private sector. As stated by the House Science Committee Chairman, the intent of HR 2413 is that information security (InfoSec) solutions should be industry led. Of equal import to the DoD is the Computer Security Enhancement Act of 1999, which mandates the employment of PKI and digital signature technologies throughout the federal government. Additional efforts on the part of the 105th and 106th Congresses include PL 105-277, Title XVII, HR 439, S 761, HR 1714, HR 1572, and HR 1685. All these bills that have passed into law address the issue of information security and use of digital signatures. Clearly, this issue has caught the interest of the Congress.

It is the Task Force's belief that deploying a secure DoD-wide virtual Intranet is not a technology issue—at its core, it is a management and policy matter. Commercial and DoD

Internet security technologies are available that can adequately address DoD's present information security requirements as well as improve the present security on the NIPRNET, SIPRNET, and similar systems. A constraint in accomplishing this goal is DoD's lack of a comprehensive, overall security architecture and deployment strategy for the DoD telecommunication systems that exist today (e.g., NIPRNET, SIPRNET, JWICS, and the like); in addition, each of the Services is pursuing its own security solutions for their tactical communications infrastructure—as discussed later in this report. The Task Force's assessment is that security is often treated more as an afterthought—a capability presumed to be available rather than addressed and incorporated at the outset of any new DoD C4ISR program or one undergoing technology refresh.

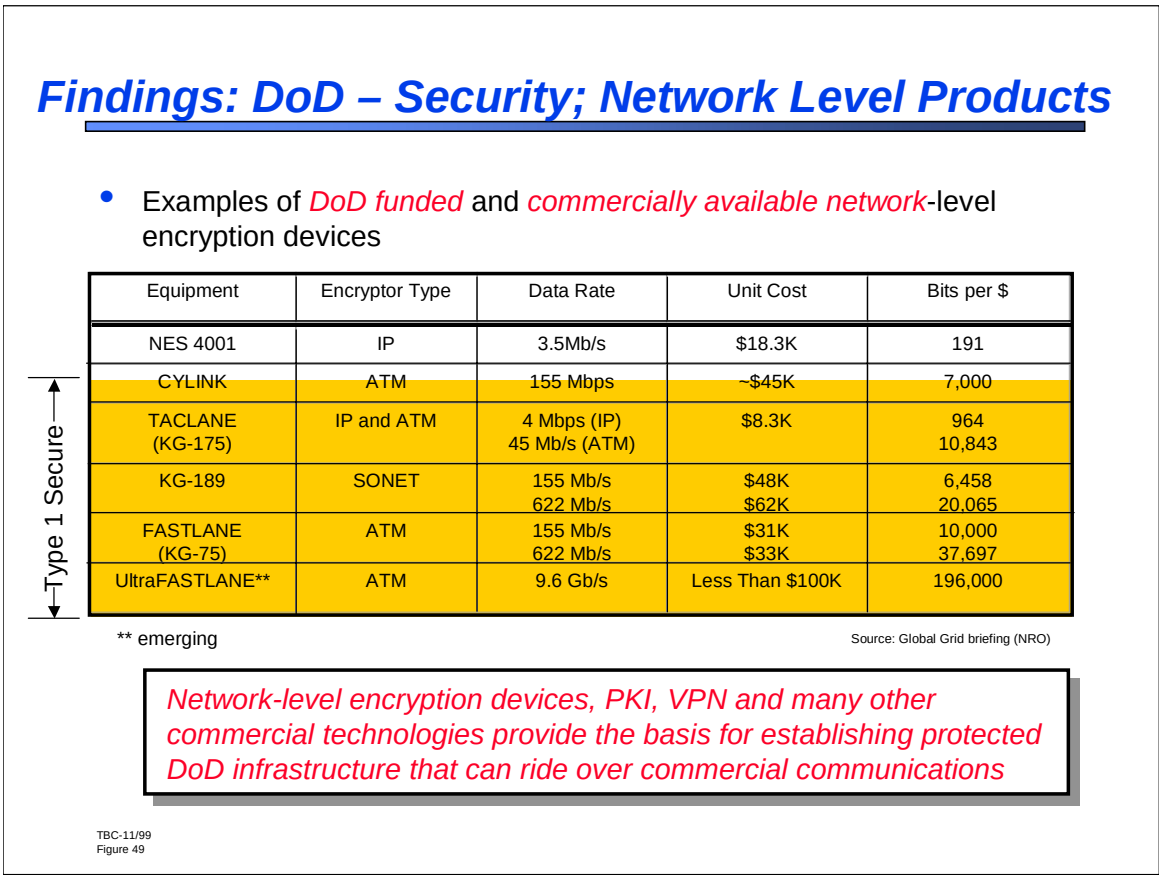
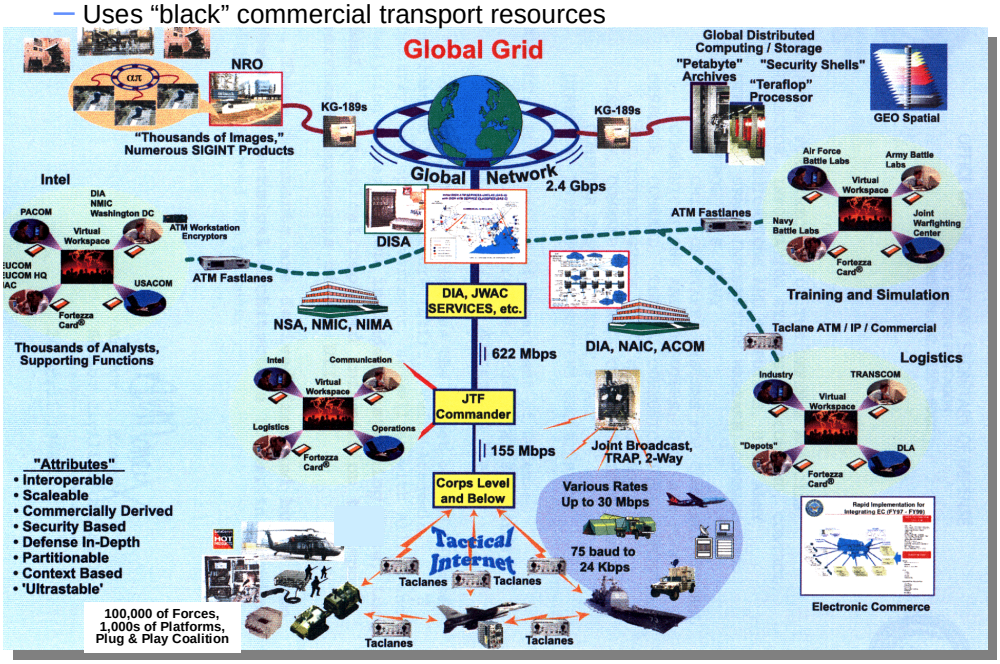


Figure 49 provides examples of DoD-funded and commercially available network-level encryption systems (NESs). Network-level encryptors, PKI, virtual private networks (VPNs), and many other commercial security technologies discussed earlier in this report provide a sound basis for establishing a protected DoD-wide virtual Intranet (GIG) that can use commercial telecommunications as transport media. The NESs provide a means of transporting classified information, at multiple levels of security, across an unsecured Internet (transport). They can also be used to secure telecommunications links. In the first case, an end-to-end (network-to-network or even host-to-host) security architecture is used, while in the latter case security is set on a link (circuit) basis—two very different security architectures with dramatically different implications in terms of being able to use private sector telecommunication resources and systems for secure DoD information transport.

Findings: DoD – Security; Internetwork Implementation

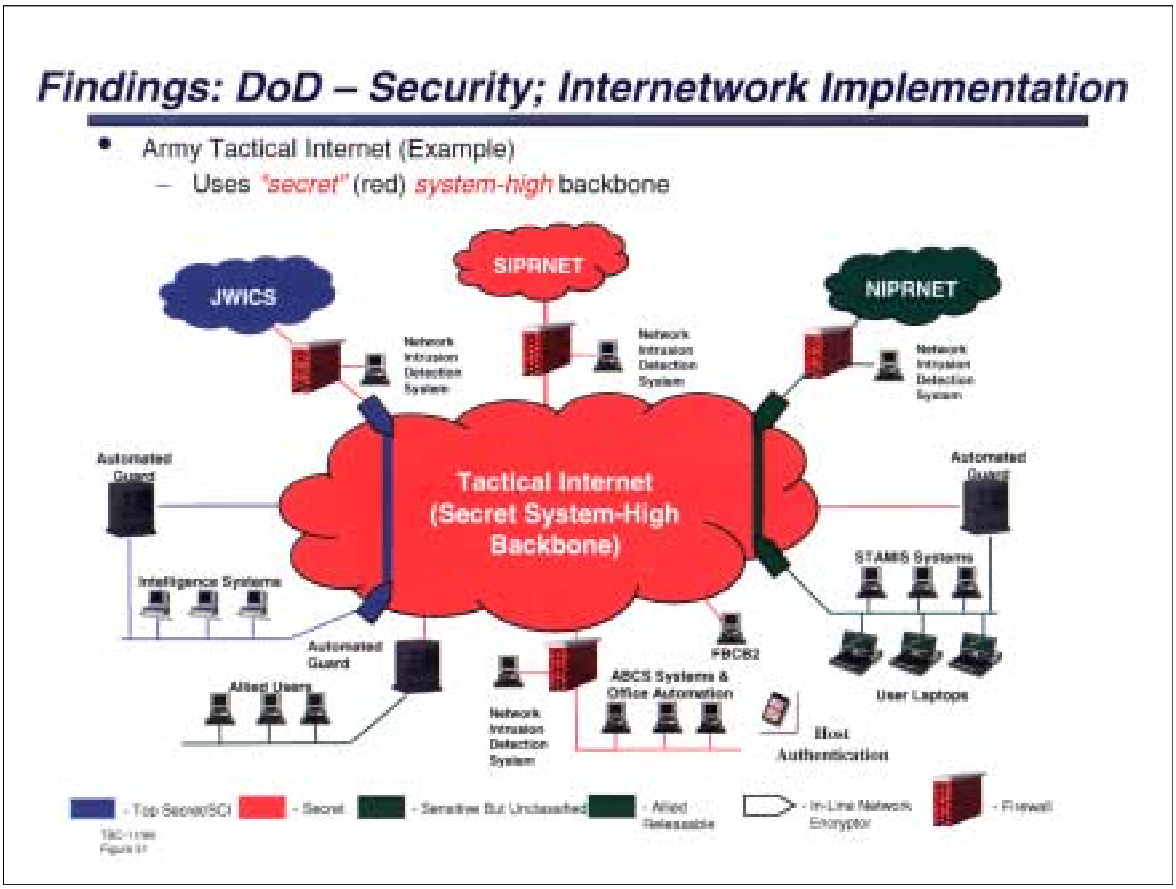
- *Secure Integrated Information Infrastructure (Example)*
  - Uses "black" commercial transport resources



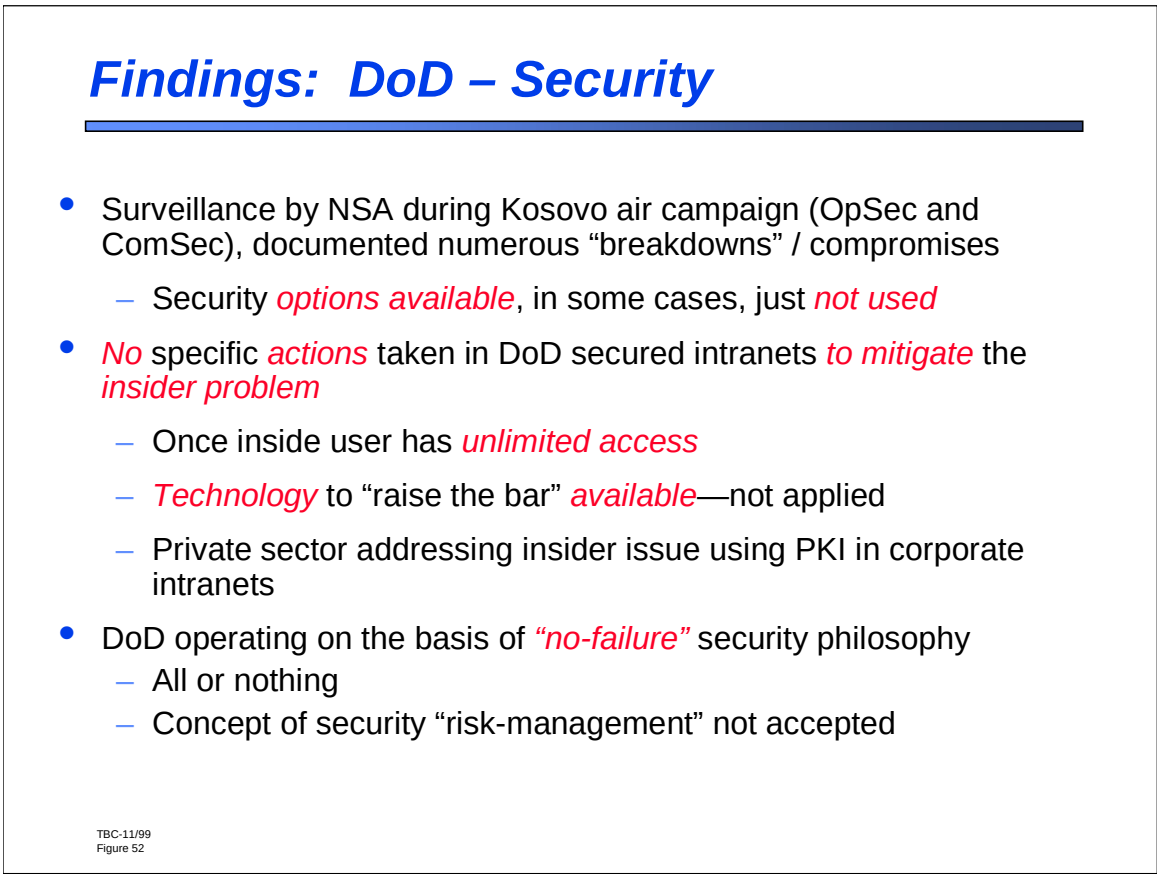
TBC-11/99
Figure 50

Figure 50 provides an example of a proposed end-to-end secured DoD Internet that employs a commercial, standards-based, ATM backbone. This concept, the NRO Global Grid discussed earlier, is intended to support intelligence dissemination across a DoD-wide virtual Intranet. At the boundaries of networks, the encryption devices noted in Figure 49 are used to partition communities of interest (at multiple levels of security) that then share a common, unsecured wide-area transport network. The resulting Intranet is a VPN segregated from a potentially broader user community through the use of the network encryption system. The segmentation of the user community, through the use of multiple levels of encryption and multiple NESs, allows the use of a common "black" telecommunications intranet between the users (whatever their locations).

Because the foundation of the Global Grid is commercial Internet standards and protocols, commercial security technology, and commercially available NESs, the community of users can include not only U.S. DoD personnel, but also users from other U.S. government agencies as well as users from allied and coalition partners. The only requirement is that they too use commercial Internet technologies. This interoperability is, of course, at the transport level. Interoperability at the application layer of the GIG would still require a common messaging system and common data elements—however, as indicated in the introduction to this report, the Task Force focused its attention only at the transport layer of a GIG.



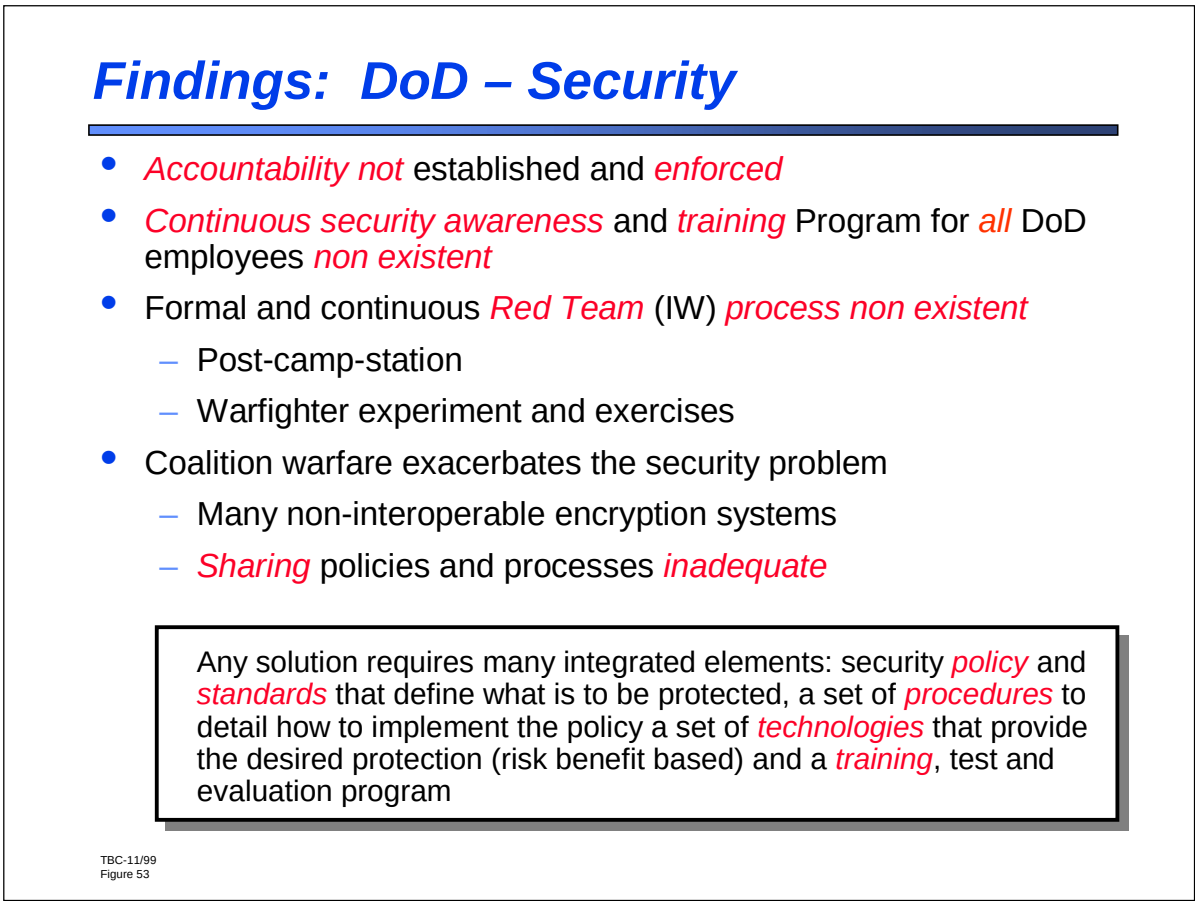
In contrast to the Global Grid end-to-end security architecture, Figure 51 shows the security architecture for the Army's Tactical Internet which uses a Red system-high backbone. Although traffic with multiple levels of security transit the backbone and are segmented with NESs and trusted guards, the Secret-level users are interfaced directly to the backbone. (Note that unclassified traffic is segregated through NESs and also transits the backbone). This security architecture implies that all links within the backbone must be protected either physically or, if wireless, through such techniques as transmission security (TRANSEC) layered under any Communication Security (COMSEC) services. In this architecture, if a node of the backbone in Figure 51 is compromised, it is very possible that all backbone-high traffic (secret in the example shown) will be compromised—the backbone nodes are red. In contrast, the backbone nodes in the Global Grid (Figure 50) are Black and can be part of the private sector telecommunications infrastructure. These two security architectures are very different and ultimately incompatible in the sense of directly connecting the Tactical Internet backbone to the Global Grid backbone.



In addition to the different communication security architectures being pursued by the Services, the Task Force noted that in recent military operations in the Balkans tactical information was compromised in several instances, due in part to incompatible communications security systems and capabilities—either between U.S. Service assets or between and amongst allies—forcing the end user to employ unsecure communication means.

Further, the Task Force noted that no specific actions are being taken to mitigate the insider threat within DoD classified Intranets. Though certain software tools are being investigated to monitor internal activity and to report suspicious access, the Task Force could not identify a DoD-wide strategy to meet this challenge. As noted earlier in this report, the private sector is developing technology to help diminish the insider threat—these technologies are available to the DoD.

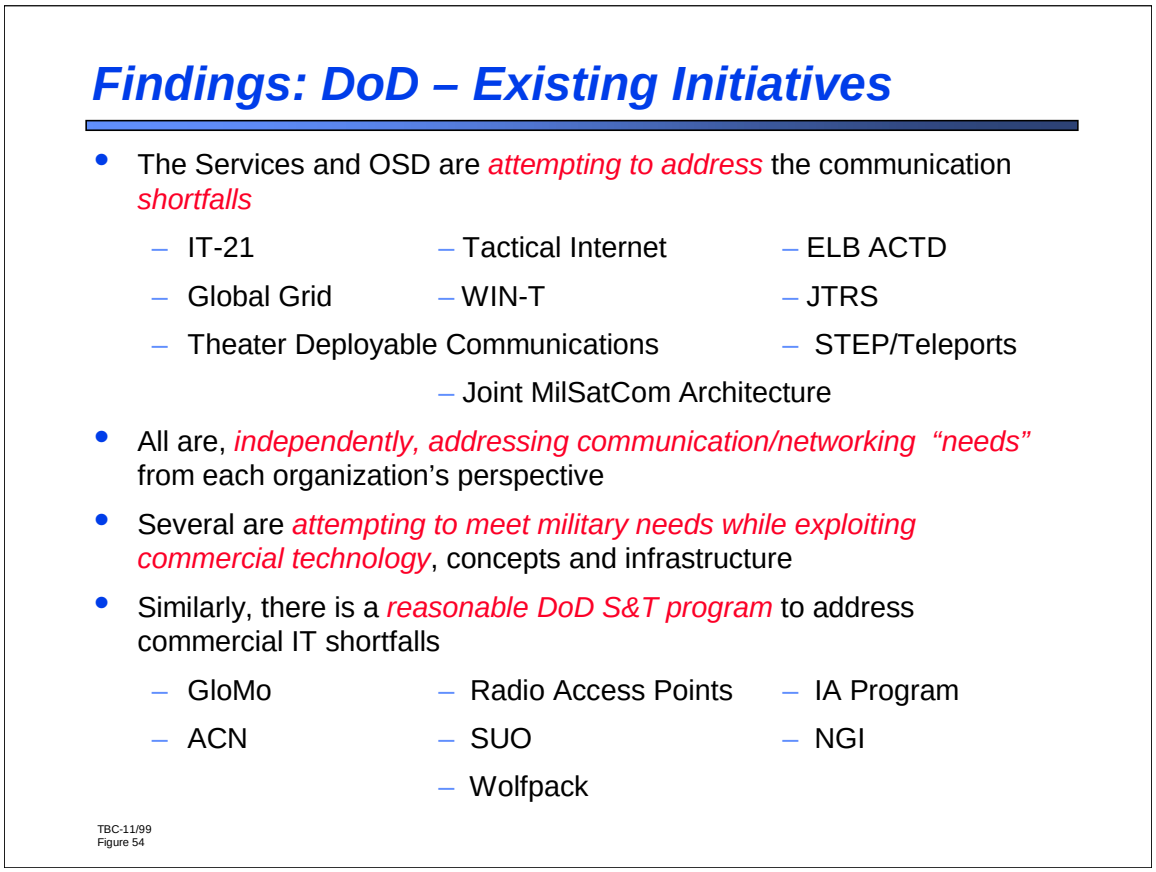
Though DoD and the Intelligence Community (IC) are in the process of transitioning to risk management as opposed to a risk avoidance security strategy (the latter being the driving goal over the past several decades), this transition as been very slow in coming to fruition and has yet to be widely accepted throughout the Department.



Finally, the Task Force noted that continuous security training and security awareness briefings for DoD personnel, so prevalent during the Cold War period, have all but disappeared from day-to-day business processes. Formal and continuous Red Team exploitation of DoD enterprise information infrastructures, recommendations made as a result of Exercise Eligible Receiver '97 and in several DSB studies, have yet to be implemented; nor is Red Team exploitation being conducted as a continuous process during warfighter experiments and exercises. If Red Team processes were set in place, they would serve to heighten security awareness at all levels all the time.

Based on the briefings received by the Task Force, the panel concluded that any DoD security solution requires many integrated elements: security policies and standards that define what information is to be protected and at what level of protection; a set of procedures to detail how to implement the policies; a set of agreed-to technologies that provide the required defense in depth (risk and cost-benefit based); and, perhaps most important, a training, test, and evaluation program.

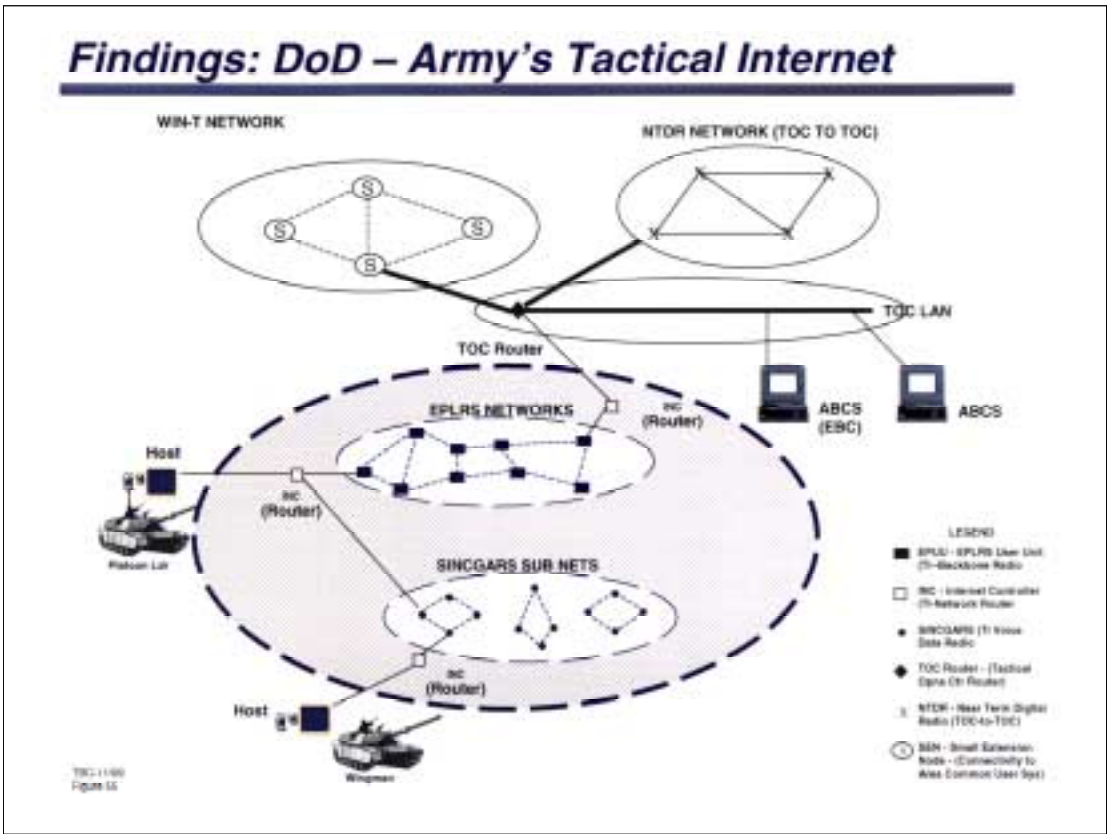
The fact that more and more U.S. military operations are being conducted in an "allied" or coalition environment furthers exacerbates the security problem. The Task Force found instances involving non-interoperable encryption systems that resulted in breakdowns in communications security to the benefit of the adversary. Furthermore, the Task Force found no consistent policies, procedures, processes, or technologies for sharing information with coalition partners.



The Task Force findings regarding the explosion in the private sector Internet technologies, the value of internetworking military telecommunications systems to increase combat effectiveness, and the impending shortfall in meeting military telecommunication needs, have not gone unnoticed by DoD and the Services. Numerous good initiatives, acquisitions, advanced technology demonstrations (ATDs) and advanced-concept technology demonstrators (ACTDs) are addressing elements of these issues. Some of these programs are in the planning or architecture development stage, others are experiments to identify the best approaches for meeting user needs, and yet others are enhancing current production and fielded systems.

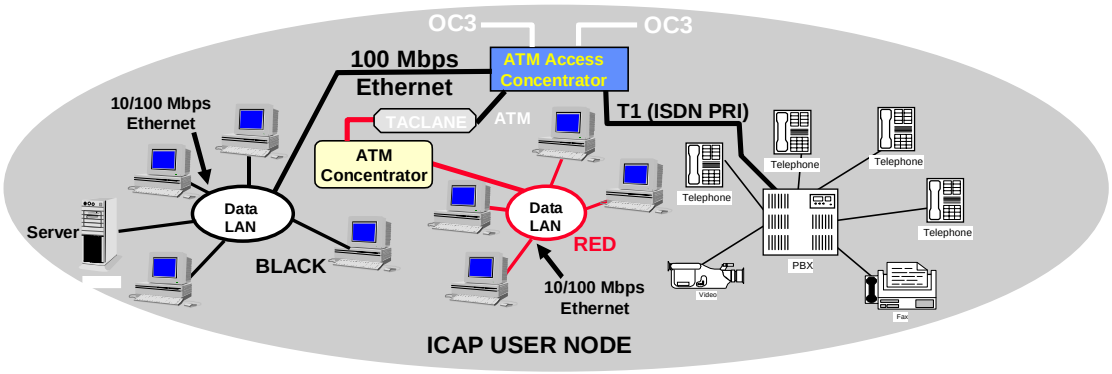
While the list in Figure 54 is not all-inclusive, it does represent a wide cross-section of ongoing activity within DoD. Each of these initiatives addresses communications shortfalls or needs from each individual sponsor's perspective, covering a full range of system types from individual products or family of products, individual systems, networked systems, and global architectures. In every case, the common theme is the leveraging of commercial concepts, technologies, and products toward satisfying individual service requirements. Commercial technologies are "adopted" in cases where direct application to a tactical military environment best satisfies the requirements, while other applications require commercial technologies to be adapted to meet tactical requirements. Only when neither adopting nor adapting commercial products and/or technologies will adequately address requirements is custom development considered.

In addition, DoD has a reasonably robust set of science and technology (S&T) programs in place to address the military shortfalls of private sector telecommunications technology. The DoD's initiatives in cost sharing with the commercial sector for the development of technologies and products where mutual interests exist appears to have been well received by industry as an effective mechanism for addressing capability shortfalls to meet both military and commercial telecommunications requirements. S&T programs are also evaluating integrated system concepts with significant leveraging of commercially available and commercially adopted technologies and products. Several of the telecommunication S&T programs focus specifically on technology areas that the private sector will not address in the near term. These areas include dynamic, peer-to-peer, multihop, wireless telecommunications; automated, adaptive spectrum usage embodied in intelligent, wireless telecommunication nodes; and information assurance in a high threat (wired or wireless) environment.



The Army's Tactical Internet is one specific example of an ongoing tactical telecommunications initiative exploiting Internet concepts and technology that will provide an integrated voice and data IP-based Intranet as part of the Army's Force XXI Digitization program. The Tactical Internet is the Army's primary tactical communications network for the warfighter; it interconnects brigade and below units and links them to higher and adjacent echelons through the Warfighter Information Network–Tactical (WIN-T). The Tactical Internet leverages commercial technologies, protocols, and products to provide secure voice and networked data services throughout the tactical battlespace by integrating legacy and commercial-based network and telecommunications systems. The Tactical Internet's use of commercially-accepted standard network interfaces and protocols enhance Joint Service and Coalition interoperability and both operational and system architecture flexibility, as well as the potential for rapid evolution of the information infrastructure as commercial technology evolves and becomes available.

Findings: DoD – AF Theater Deployable Comm (Future)



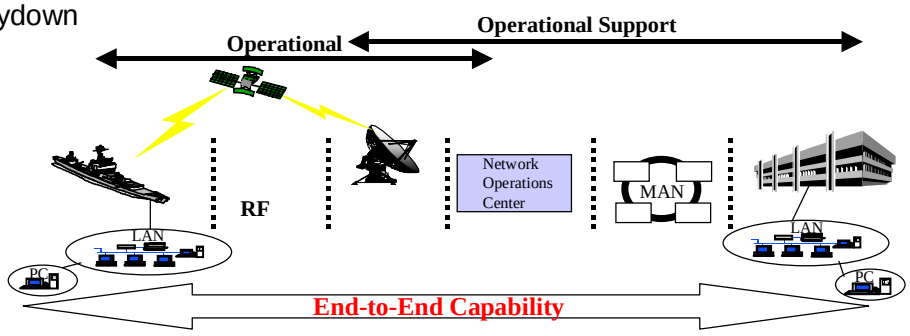
- *Secured,* Internet-Protocol-based *internetwork*
- Integrates *Multiple Levels of Security* on common transport network
- Provides *integrated* voice, video and data *services*
- Leverages *commercial technology*

TBC-11/99
Figure 56

The Air Force's Theater Deployable Communications (TDC) system is another example of a tactical telecommunications initiative to provide voice and IP-based data connectivity to the deployed user. The Integrated Communications Access Package (ICAP) component of TDC leverages commercial technologies and products to provide secure voice, video and data services to the tactical battlespace with long-haul telecommunications reachback to sustaining-base systems. Through the use of commercial Internet standards and protocols, the TDC could provide the AF with greater interoperability and architectural flexibility when fighting jointly with other forces that use the same standards.

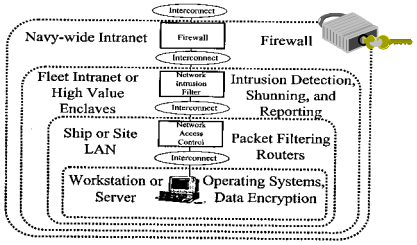
Findings: DoD – Navy IT-21

- Provides *Internet Protocol* (IP) based internetwork for *afloat, ashore* and *mobile* Naval forces
- Laydown



- *Infrastructure is secure/reliable*
- Leverages *commercial technology*

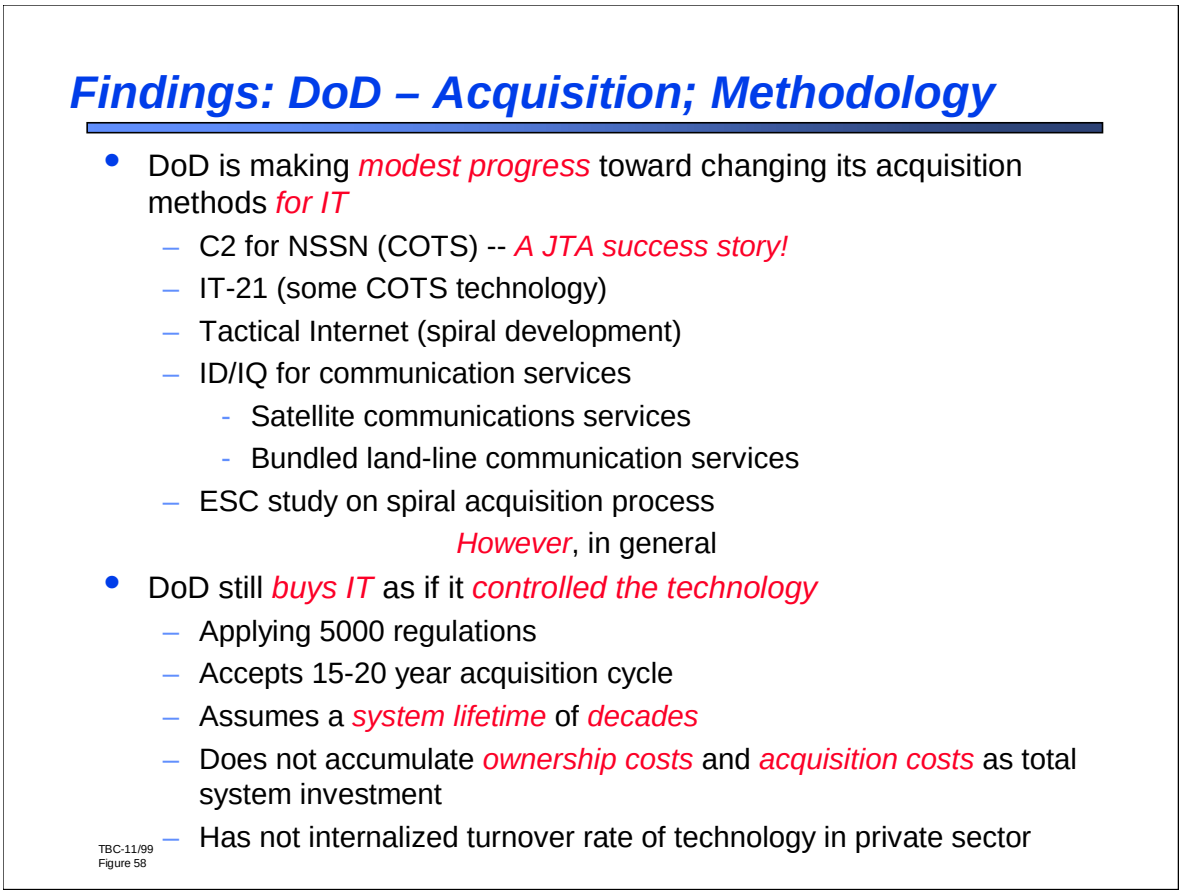
Defense-in-depth



TBC-11/99
Figure 57

Finally, the Navy's telecommunications initiative under IT-21 is expected to provide secure IP-based internetworked services from ashore to the deployed user both afloat and mobile. Like the other Services' examples, IT-21 also leverages commercial Internet and telecommunications technologies and products to provide end-to-end operational and operational support information services and connectivity throughout the battlespace. Reliability, security, user-friendliness, and interoperability are guiding principles of IT-21 in its effort to support the goal of a single computer on a desktop providing integrated tactical and tactical-support information services.

In each of these three Service examples, the common themes are exploitation of commercial telecommunications and Internet technologies, augmenting military telecommunications to meet warfighter needs and internetworking the Services' infrastructure to increase combat effectiveness. It is interesting to note, though, that the Services are pursuing similar objects but their approaches, when looked at in depth, are sufficiently different in architecture and implementation details that interoperability, from a joint perspective, is more difficult than is necessary or desirable. Differences in security architectures, internetwork management approaches, IP naming and addressing conventions, and differing extensions to commercial protocols and standards make the formation, deployment, and fighting of joint task forces (with allied and coalition partners) complex and ad hoc—a situation that can be greatly improved with agreement between, oversight for, and joint leadership of these and numerous other Service telecommunication initiatives.

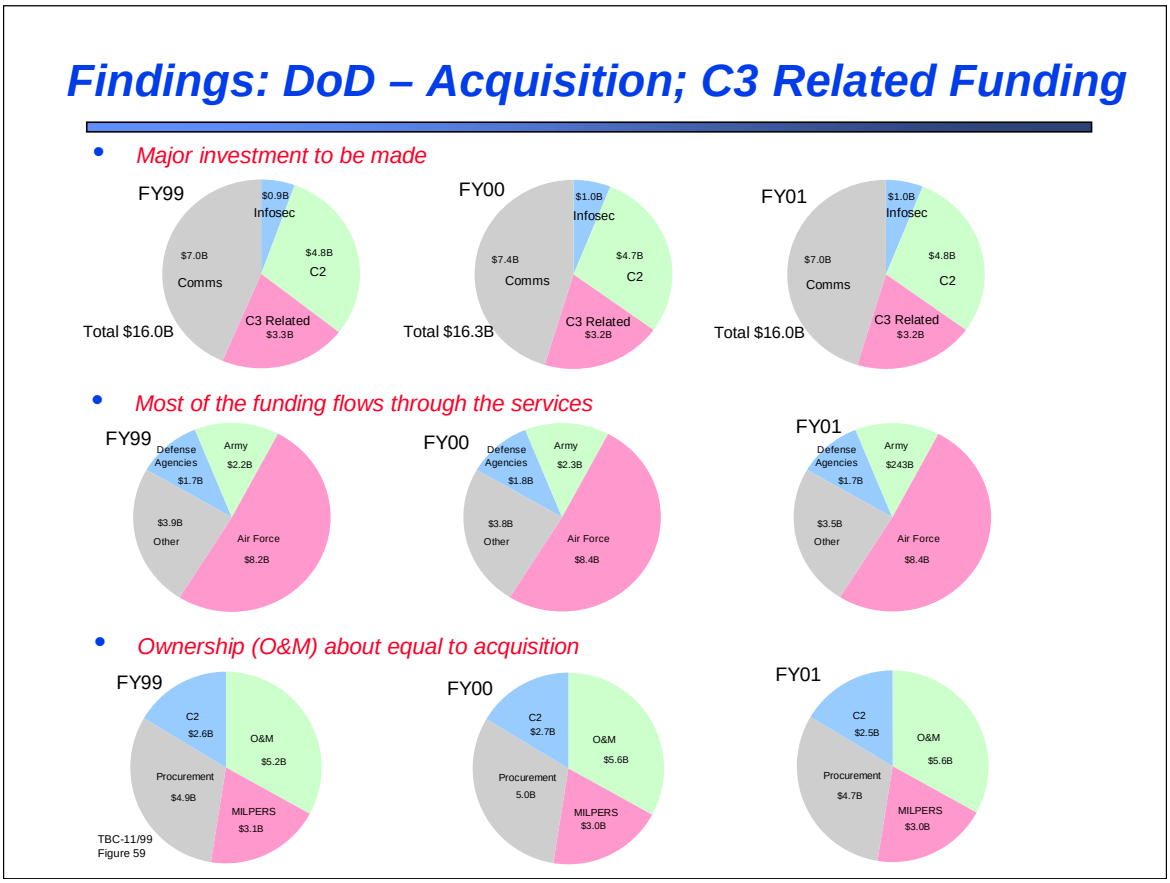


The Service initiatives noted are all attempting to exploit commercial telecommunication systems and technologies through several creative, rapid acquisition programs. The spiral acquisition approach used for the Tactical Internet, and addressed in depth in a study by the Electronic System Command (ESC), is an example of a creative approach to bringing critically needed IT capabilities rapidly into the Services. Similarly, the acquisition strategy for the C2 suite of hardware/software for the Next generation Subsurface Combatant Nuclear submarine (NSSN) is a JTA success—standards-based commercial-off-the-shelf processing technologies are being integrated and delivered to the Navy in a very short time frame and at significant cost savings when compared to prior SSN C2 systems procured through more traditional DoD acquisition processes.

These aforementioned acquisition initiatives are, however, exceptions rather than standard practice for acquiring the IT (including telecommunications) capabilities needed by our Services and CINCs. In general, our acquisition practices for IT are still based on processes established during the Cold-War era. The traditional, incremental model of acquisition was developed in a relatively stable era of known threats; the enemy's moves were fairly predictable and long-term programs could be structured and funded to ponderously, but reliably, overcome formidable technical problems. Such a model is not well suited to rapidly changing, multipolar geopolitics, and will tend to lag behind both technological advances *and* changes in the threat environment. The average cycle time (from program start to initial operational capability [IOC]) for all programs begun between 1970 and 1992 is slightly over nine years. Pre-1992 programs

providing Selected Acquisition Reports (SARs) during the 1996 reporting period indicate an even higher average time of 11 years. Many efforts last far longer; some achieve IOC only after fifteen to twenty years of work. One legacy C3 program is the Single Channel Ground and Airborne Radio System (SINCGARS) which began in 1974, and is currently being completed with the procurement of the remainder of 300,000 radios by fielding radios to the reserve and National Guard units. The same situation exists with regard to the C2 systems being developed for our forces. In most cases, the C2 systems we will be deploying in the near future have been in development for over 15 years—many are based on 10-year-old IT.

This C2 cycle time is inconsistent with the rapid turnover of IT in the private sector, where generations of certain technologies last only two years. The emerging threats, transnational and nation-state, have access to or are exploiting these technologies. In this respect, the DoD acquisition process places our warfighter at a disadvantage.



The acquisition of commercial IT and services by DoD is not primarily hindered by lack of resources. As shown in Figure 59, the actual budget in FY 1999 for C3 programs is $16 Billion, and reflects an increase in the total baseline cost of C3 programs, when compared with previous years. The largest adjustment to the C3 baseline cost was the transfer of funds for the Joint Surveillance Target Attack Radar System (JSTARS) from Tactical Intelligence and Related Activities (TIARA) to the C3 area. This transfer increased the C3 baseline by over $800 Million in some years.

For FY 2000, the DoD budget request for C3 programs totals $16.3 Billion. This increase in funding for C3 programs is attributable primarily to increased operations and maintenance funding to sustain the readiness of the Department's current C3 capabilities, as well as a slight increase in procurement funding to modernize the Department's C3 capabilities. Total funding for C3 is projected to return to $16 Billion in FY 2001.

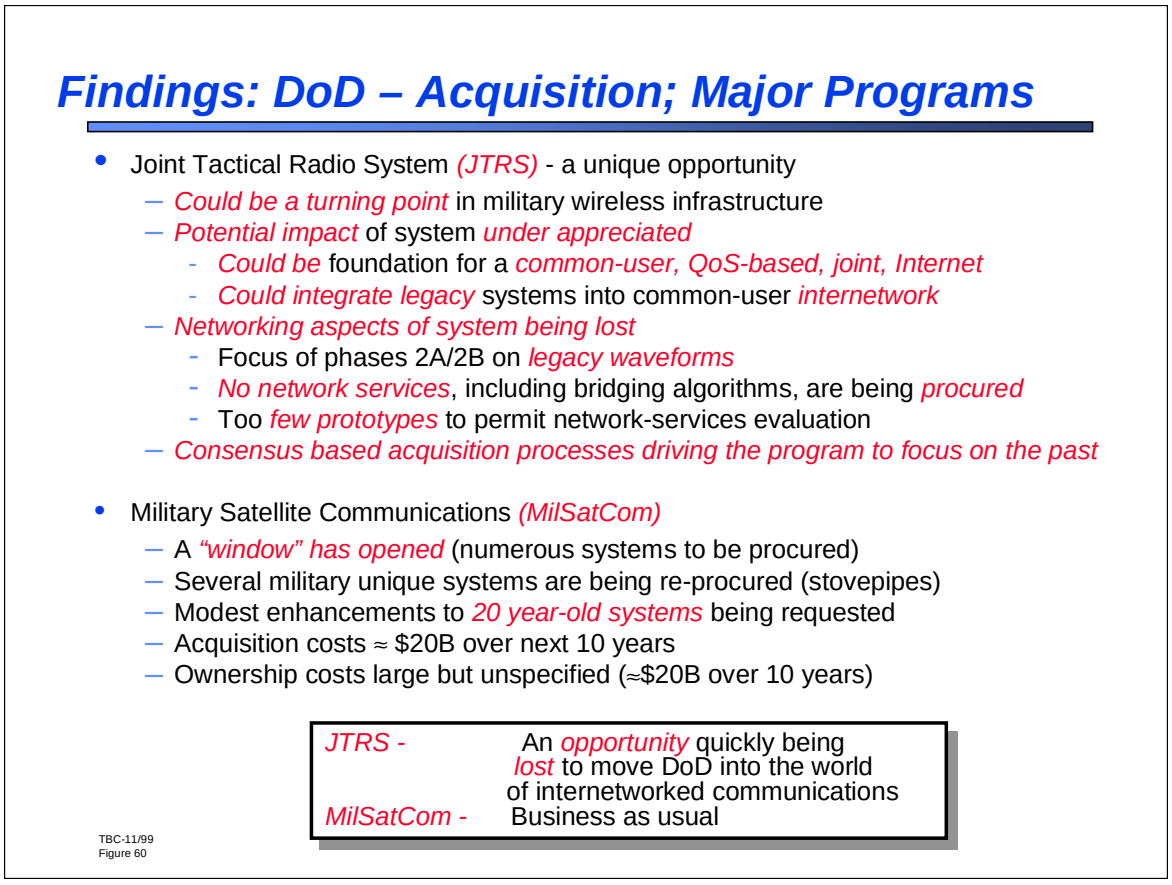
The central focus of C2 is on the decision-maker. Decision-makers operate within a framework of established doctrine, strategies, tactics, and procedures and are supported by an array of C2 systems. These systems consist of the facilities, decision support systems, and C2 equipment essential to a commander for planning, directing, coordinating, and controlling the operations of their assigned forces. These programs address the broad range of C2 capabilities needed to command and control both strategic and conventional forces. This includes support at all levels of command, from the National Command Authorities through the joint/tactical

operations echelons and down to front-line tactical elements. In the FY 2000–2001 budget request for C3, a total of $4.7 billion is requested in FY2000 and $4.8 billion is projected in FY2001 for the C2 area.

Communications programs provide a Defense Information Infrastructure (DII) that connects DoD mission support, C2, and intelligence systems and users through voice, data, imagery, video, and multimedia services. These capabilities include fixed-base communications infrastructure, long-haul communications via government-owned or leased terrestrial facilities, MilSatCom necessary for global end-to-end information connectivity, theater deployable communications, and tactical transmission systems that allow warfighters to exchange information while on the move wherever they may be located. In the FY2000-2001 budget request for C3, a total of $7.4 Billion is requested in FY2000 and $7 Billion is projected in FY 2001 for the communications area.

The DoD yearly acquisition funds for communication and C2 systems are significant. It is also interesting to note that the operations and maintenance costs of these systems are nearly equal to the funds available for acquisition of new technology. Furthermore, military personnel supporting this C3 infrastructure are a very significant element of the total costs.

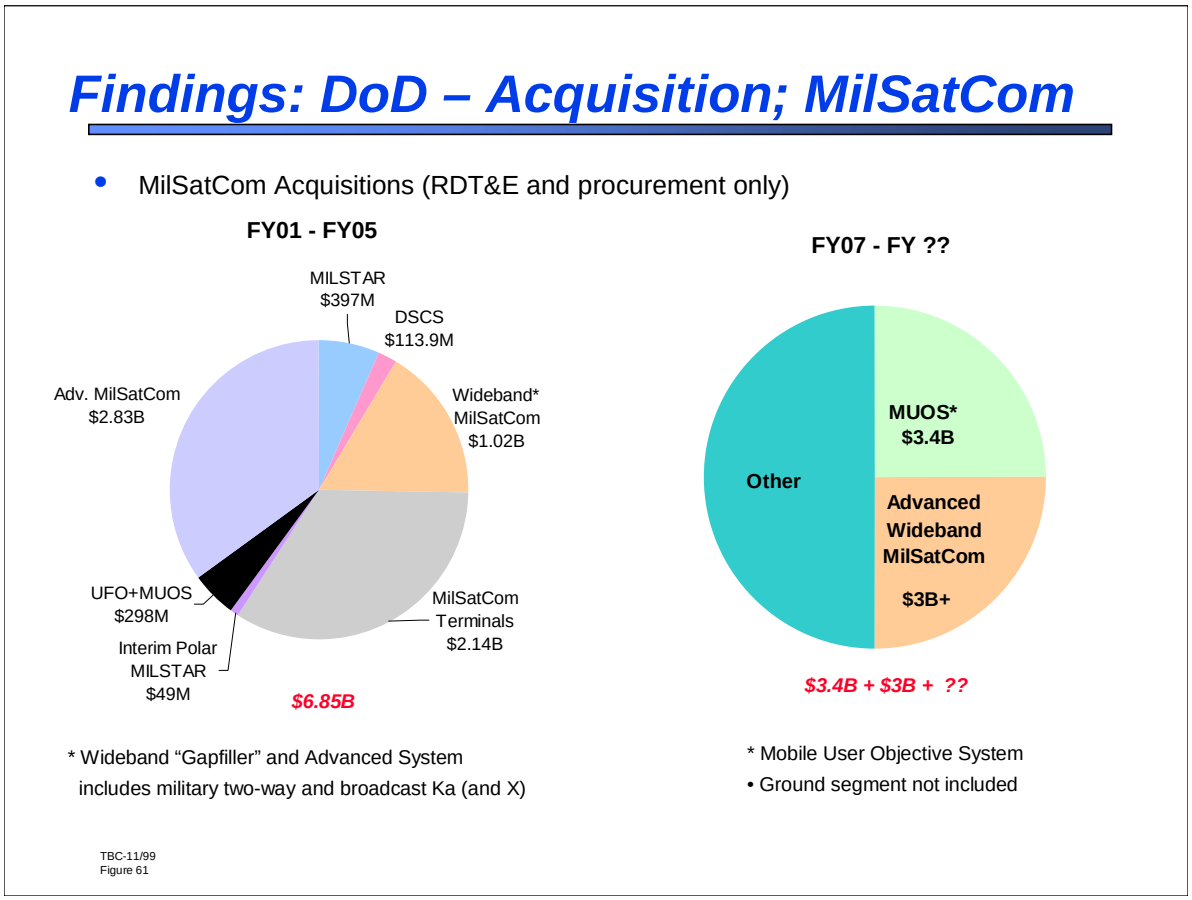
In contrast to the Task Force's findings regarding the acquisition and capitalization of IT and telecommunication services in the private sector, DoD acquires C3 infrastructure over tens of years and retains these systems in the inventory for decades. In the private sector, recapitalization of C3 type infrastructure occurs on the order of every five to eight years. In DoD the user devices are expensive to acquire and own. In the private sector, the user devices are very inexpensive and rapidly replaced (in one to three years). Finally, in DoD the customers (the CINCs) do not drive the C3 acquisition process—the Services acquire the infrastructure to meet their respective needs; the CINCs are the recipient of the technology. In the private sector, the customer drives the technology flywheel. In both sectors, significant investments in telecommunications systems and services are made every year.



Examples of two major development and/or acquisition programs presently underway within DoD are the Joint Tactical Radio System and the Military Satellite Communication systems (Figure 60). The JTRS concept was developed as a result of the Decision Support Center (DCS) studies on the value of internetworking military platform/system (Figures 42 through 44). As discussed earlier in this report, internetworking resulted in greatly enhanced military operational capabilities—JTRS was intended to be a family of network-based telecommunication nodes that would act as network bridges among developed legacy radios and at the same time offer increased telecommunication services (capacity) to our warfighters. However, the Task Force noted that the internetworking aspects of the program, a critical contribution to moving the DoD point-to-point and broadcast wireless infrastructure into an integrated internetwork, is not being adequately addressed (see Annex D). Furthermore, Service-specific interests are forcing the JTRS program to focus on the many Service radio legacy waveforms, and political and Service interests are causing waivers to be sought that will introduce more legacy systems and waveforms into the existing warfighters' telecommunication infrastructure.

Such pressures on the JTRS program reflect the difficulties in the DoD consensus-based management process for programs such as this one. A critically important transition for DoD wireless telecommunications is being put at risk by our inability to embrace a vision, concept, and program to meet the integrated requirements of our CINCs.

Similarly, the MilSatCom systems DoD is considering procuring in the future are incremental extensions of prior DoD systems. Although DoD's investment over the next 10 years for space-based telecommunications will be very substantial, the value returned in the context of meeting growing warfighter needs for high capacity reach-back and reach-forward telecommunications will not be satisfied (Figure 31). Furthermore, the DoD MilSatCom acquisition strategy does not address the exploitation of emerging private-sector space-based telecommunications technology, nor does the DoD strategy address, in depth, how to integrate whatever space-based telecommunications resources it acquires into an integrated DoD-wide virtual Intranet.



That is not to say, however, that significant effort and attention is not being focused on MilSatCom. Language in the FY 1999–2003 Defense Program Guidance (DPG) directed that the Under Secretary for Acquisition and Technology, the Chairman of the Joint Chiefs of Staff, and the Assistant Secretary for Command, Control, Communications, and Intelligence provide the Deputy Secretary "a SatCom integrated framework, to include an implementation schedule and developmental tasking, that addresses the recommendations of the MilSatCom Transition Working Group, as approved by the Joint Space Management Board (JSMB). This integrated framework will be based on the Joint Requirements Oversight Council (JROC) validated Advanced MilSatCom Capstone Requirements Document (CRD), when available."

The DoD currently operates three types of MilSatCom systems to support the warfighter and national requirements. Each of these systems satisfies specific requirements:

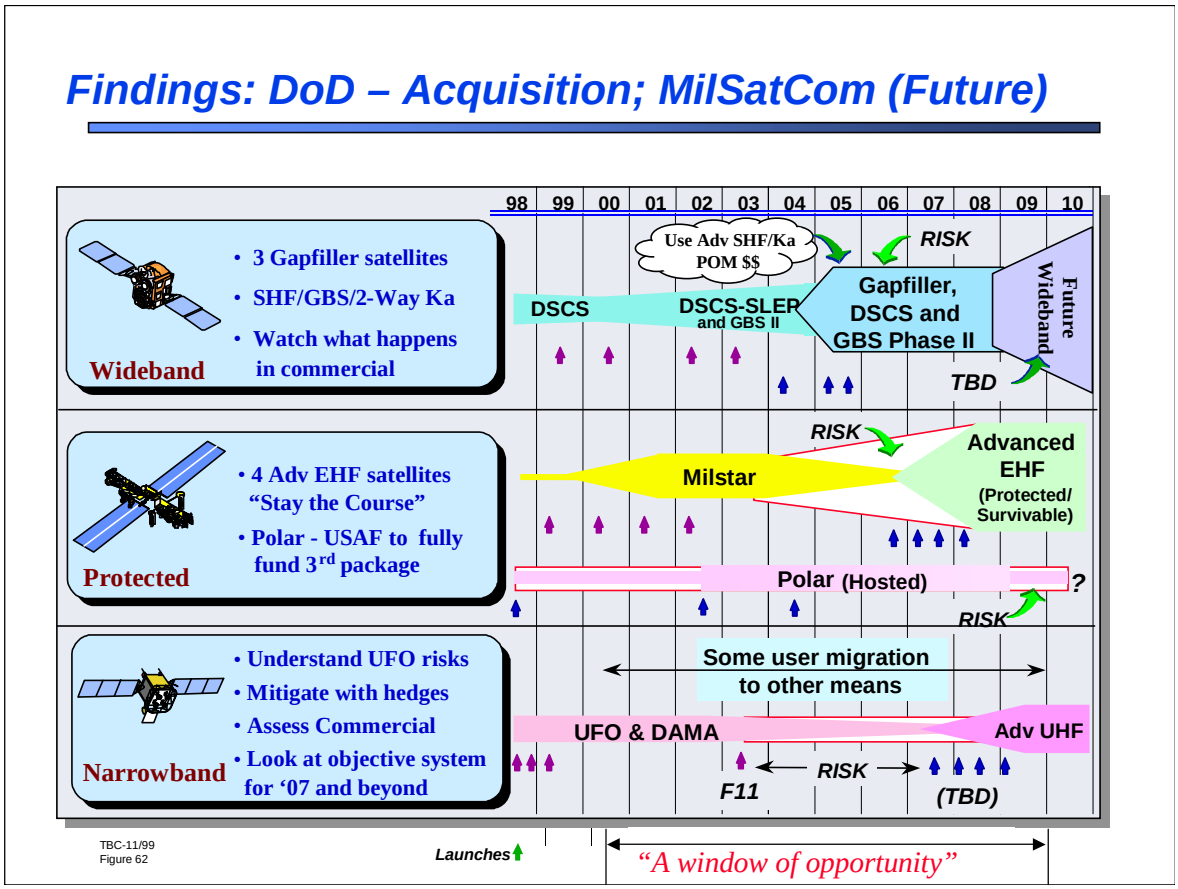
Protected Communications: Protected systems provide the warfighter and national elements with secure, assured, and survivable communications. This requirement is unique with no current commercial equivalent. The Milstar System satisfies this requirement using the EHF frequency band.

Wideband Communications: Wideband systems support the movement of large quantities of data including video, imagery, and large databases. The Defense Satellite Communications System (DSCS) satisfies this requirement using X-band frequencies.

Mobile Communications: Mobile communication systems provide networked multi-party and point-to-point narrowband links to tens of thousands of rapidly moving, disadvantaged warfighters. The UHF Follow-On System (UFO) satisfies this requirement using the UHF band.

To address the DoD's rapidly growing information needs for the 21st century as well as the normal replacement of these systems, the DoD Space Architect's Office developed the Department's future MilSatCom architecture. This architecture establishes clear direction for migrating users to these three general classes of service supported on separate satellite systems. The DoD Space Architect's Office has been realigned under the Assistant Secretary of Defense C3I and renamed the National Security Space Architect's Office.

In August 1996, the Joint Space Management Board (JSMB) approved, in concept, the architecture objectives, goals, and strategy, with the understanding that long-term resource decisions would be predicated upon a cost-constrained requirements study. The JSMB tasked the Deputy Under Secretary of Defense (Space) to lead the DoD effort to refine the future MilSatCom architecture and develop an affordable transition strategy. The Deputy Under Secretary of Defense (Space)–led MilSatCom Senior Steering Group (SSG), together with the U.S. Space Command-led Senior Warfighter's Forum, recommended a transition strategy that was endorsed by the Joint Requirements Oversight Council (JROC) in October 1997. The Advanced MilSatCom Capstone Requirements Document (CRD) was approved by the JROC in April 1998. The JSMB has been replaced by The National Security Space Steering Group and The Deputy Under Secretary of Defense (Space) responsibilities have been realigned under the Assistant Secretary of Defense C3I.



As shown in Figure 62, the strategy for protected communications calls for launching today's three remaining Milstar II satellites as planned through 2002, followed by a more capable advanced system starting in 2006. The Air Force is the executive agent for the Advanced Extremely High Frequency (EHF) system and has completed the initial joint program Operational Requirements Document (ORD). Milestone I acquisition approval was obtained for this Acquisition Category (ACAT 1D) program in early 1999; Milestone II/III is planned for early 2001. North polar coverage for protected communications will continue to be provided by packages hosted on polar orbiting satellites. Acquisition of the polar-orbiting packages continues consistent with the host spacecraft's schedule.

The strategy for wideband communications calls for launching today's four remaining DSCS Service Life Enhancement Program (SLEP) satellites as planned through 2003, supplemented by the Global Broadcast Service (GBS) packages on the last three UFO satellites. The USD/AT&L and the Joint Requirements Oversight Council endorsed the launch of an additional three commercial-type Wideband Gapfiller Satellites starting in 2004 to reduce the growing gap between tactical wideband requirements and capabilities. The USD/AT&L reviewed and approved this ACAT 1D program fall 1999. The Air Force is leading the development of the joint program ORD this fall; ORD approval is planned for early 2000.

Milestone II/III acquisition approval is planned for mid-2000. A more capable commercial-type advanced wideband system is envisioned to start in 2008.

The strategy for mobile communications calls for launching today's one remaining UFO satellite as planned in 1999, procuring another UFO satellite for launch in 2003 to fill a projected gap in capability, and launching the first new satellite of an "objective" system in 2007. The Navy is still refining details of the mobile communications transition and objective strategies.

A tenet of the future architecture and transition strategy is to reduce costs by leveraging commercial SatCom products and technology through commercial-like procurements, commercial hardware and software, and possible future innovative approaches to leasing and partnering with commercial vendors. To enable more commercial-like acquisitions for future wideband and mobile systems, users requiring protected communications will be migrated from existing DSCS and processed UFO systems to the new protected Milstar system currently being deployed.

As this strategy was briefed to the Task Force, it was noted that although interest is expressed in exploiting emerging commercial, space-based telecommunications technology, *in many cases* there were many "emotional" arguments were made that doing so is not appropriate. In several cases cost comparisons were cited; for example, between MUOS and Teledesic—as reasons that a DoD system is a better acquisition. The Task Force noted that this comparison is contrasting a very narrowband system with a very high-capacity broadband system—an ill-founded comparison at best. The Task Force does appreciate the difficulties in comparing a DoD-developed, -owned and -operated space-based telecommunication systems with those that will emerge in the near future in the private sector. The trade space is complicated and future developments in the private sector are unclear. However, the Task Force noted that a window of opportunity exists before DoD procures systems like MUOS beyond 2005. Detailed tradeoff studies should be conducted by independent organizations to address the issue of *not if but how*, commercial space-based technologies should be utilized by DoD to meet, in a systematic manner, the growing telecommunications needs of our warfighters.

Findings: DoD – Acquisition; MilSatCom

System	Class	IOC Date	Min. Terminal Antenna Dia (m)	MRC Capacity (Mbps)*	2 MTW Capacity (Mbps)**	SV Cost (est, $M)	Gnd Infr Cost (est, $M)	Lnch Cost (est, $M)	Main Cost (est, $M)	RDTE Cost (est, $M)	Total Cost	Cost to date	Inc Cost	$/bps (2 MTW)
Milstar (EHF)	Mil GEO (Protected)	1994	1	49.6	99.2	800	800	934	450		5384	4261	1123.5	$54.27/bps
Milstar (Adv EHF)	Mil GEO (Protected)	2006	1	400	800	400	800	600	450	1000	4450	0	4450	$5.56/bps
DSCS 3B (X Band)	Mil GEO (not Prot.)	1992	3.7	150	300	150	800	234	450		2084	1970	114	$6.95/bps
Gapfiller (Ka Band)	Mil GEO (not Prot.)	2004	1.8	700	1400	150	800	175.5	450	550	2425.5	0	2425.5	$1.73/bps
MUOS/UFO (UHF)	Mil GEO (not Prot.)	1993	whip	0.25	0.5	120	800	604.6	450	1100	3434.6	0	3434.6	$6,869.20/bps

* MRC geographic region = 320 Km diameter ** MTW geographic region = 3200 Km diameter

- Observations:
  - Future *protected bps* will cost *10X commercial* wideband systems
  - *Military wideband bps* cost *2X to 3X commercial wideband*
  - *Military UHF bps* costs *200X commercial* mobile bps
  - DoD *ground terminal* and *ownership/maintenance costs* make comparisons even *more disproportionate*

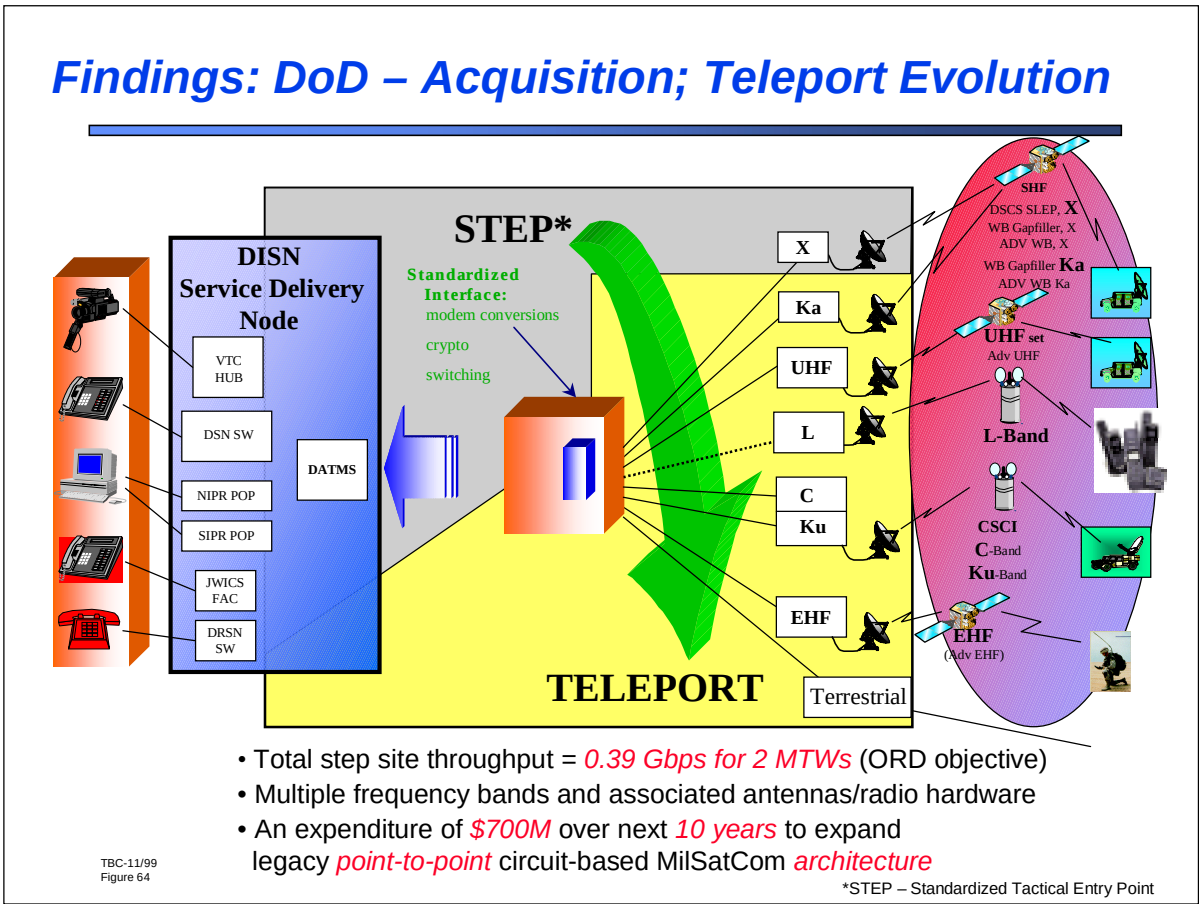
TBC-11/99
Figure 63

These trade-off studies must be comprehensive and must be updated as commercial technologies are actually delivered to the market place. The Task Force did conduct a very simple analysis to compare the systems DoD is, or plans to, acquire as part of the MilSatCom strategy to the commercial systems characterized in Figure 18. Corresponding data for the MilSatCom systems is provided in Figure 63. In this figure, space vehicle (SV), Teleport or Gateway (Gnd Infr), Launch (Lnch), Maintenance (Main) and RDT&E costs are explicitly included. Incremental costs are also shown because several of these systems have "sunk" costs already incurred. As in the commercial cases, costs are compared on a normalized $/bps basis.

It is interesting to observe that *total* system costs for military systems and for commercial systems are all approximately the same. System capacities are generally lower in military systems because they are optimized for particular, military-unique requirements such as hardening, jam resistance, or disadvantaged terminal operation. A comparison of Figures 18 and 63, shows that the cost per bps for protected data transport is 10 times the cost of bulk wideband data on a military system, and that of military dedicated wideband data is twice to three times the cost of wideband data on comparable commercial systems. This data suggests that a military-specific satellite system is appropriate only where a unique requirement is levied on the system. In other cases, it appears to be more appropriate to use an off-the-shelf commercial system either acquired by DoD or bandwidth leased from the service provider owning that system. The choice

of commercial leasing versus buying, compared to DoD design, development and ownership of unique military systems, adds to the complexity of the trade-off analysis.

Another interesting comparison between the data shown in Figures 63 and 18 is the capacity each system can provide within a geographic area equivalent to one MRC or two MTWs. In most cases, the commercial equivalent system provides greater capacity into these geographic areas. This increase in capacity has some very significant implications regarding force maneuverability and combat effectiveness. For example, a Teledesic user terminal, of about 0.6m diameter provides 20 Mbps uplink capacity. If such terminals were integrated with WIN-T nodes, the nodes would not need to be set up with terrestrial point-to-point microwave links between them. Information routing between the nodes would occur through an internetwork of which Teledesic is one network. With appropriate antenna design, the WIN-T nodes could even operate on the move. Again, a careful internetwork design and trade-off analysis is required to assess the viability of a highly internetworked, commercial technology-based DoD Intranet providing such services—clearly a creative approach to this issue could result in immense payoffs.

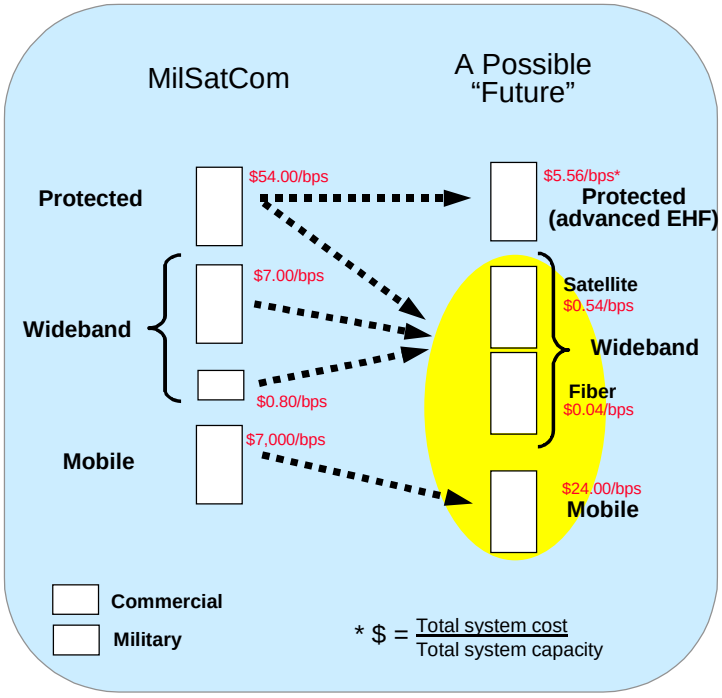


Pursuing the Teledesic discussion further, the Task Force noted that the system concept promotes the idea of switching user traffic between satellites—at most two (one for backup) ground entry points are necessary to control the satellite constellation and to provide entry into the terrestrial component of the Internet. This vision should be contrasted to the strategy DoD is pursuing whereby seven teleport sites will be acquired and strategically deployed worldwide. These sites are estimated to cost (O&M included) about $100 Million each. The sites will provide the ground entry points for the anticipated DoD MilSatCom systems, as depicted in Figure 64.

The Task Force noted that the teleports will have large antenna farms to support the many frequencies over which the MilSatCom systems operate and that the architecture for the sites (as presented to the Task Force) is circuit based and point-to-point in nature. Each satellite system provides independent circuits from subscribers that transit the teleport site independently; the total throughput for two MTWs that a site can support is 0.39 Gbps (as noted in the Operational Requirements Document for the system).

Thus, the Teleport perpetuates the stovepipe nature of the DoD satellite system, and the sites can handle only a small fraction of the anticipated space-based telecommunication capacity that two MTWs are projected to generate by 2010. Here again, the Task Force notes that a careful and in-depth trade-off study is needed to address what the Global Information Grid or DoD-wide virtual Intranet should have in place by 2010. To the Task Force, the present DoD acquisition strategy and systems do not appear able to meet the warfighters telecommunications requirements, now or in the future.

Findings: Space Telecommunications; What Might Be



- *Multiple* commercial *systems* could provide capacity and *survivability* through redundancy to allow formerly *protected DoD* communications to *transit commercial systems*
- Emerging *commercial* SatCom and fiber infrastructure *provides a cost* effective *alternative* for *non-protected* wideband *MilSatCom*
- *Purchased* commercial mobile *systems* (DoD owned) would provide capacity at approximately *$24.00/bps*
- Must be internetworked with terrestrial fiber and wireless ground-based systems

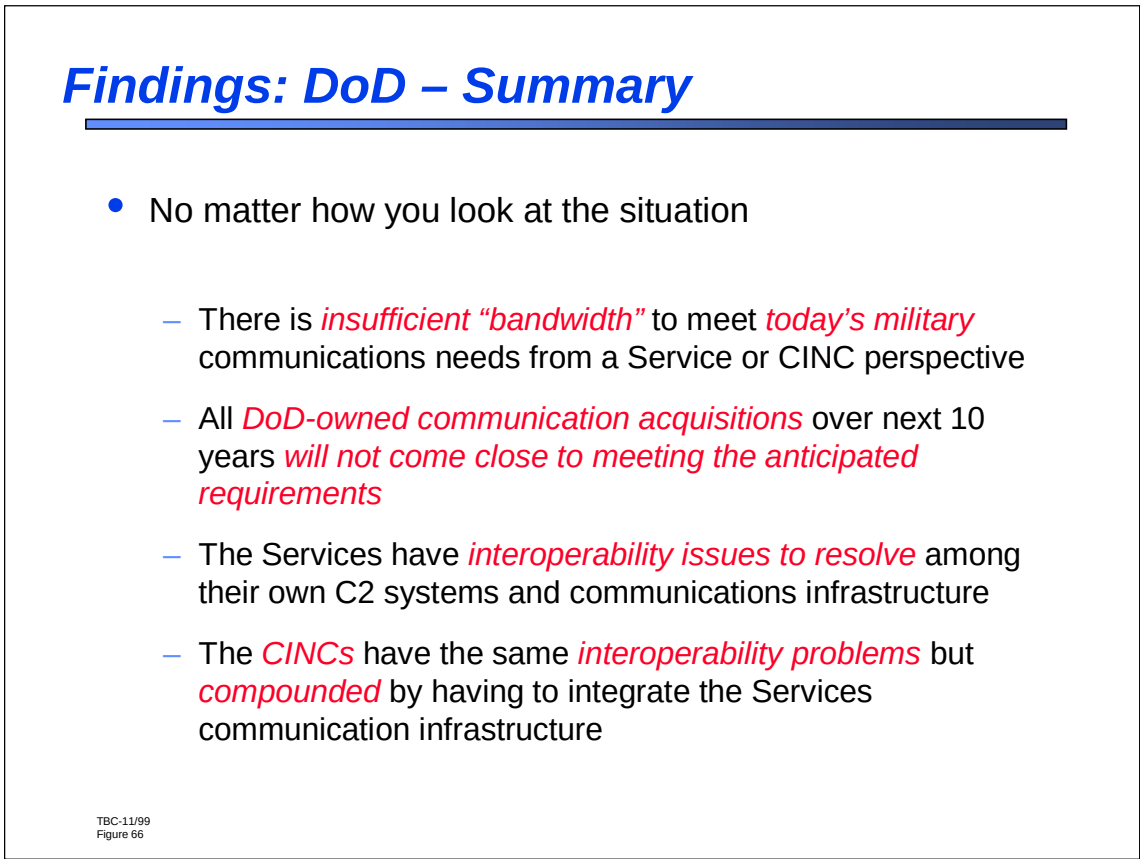
Combining its findings from the DoD and private sector, the Task Force notes that there appear to be two factors that could significantly influence DoD's MilSatCom strategy: (1) the growing gap in military telecommunication requirements versus DoD systems' ability to meet them, and (2) the growing disparity in costs between MilSatCom systems and commercial satellite and fiber-optic systems. The Task Force recognizes the unique military need for a highly protected, minimum essential DoD communications network. Commercial systems will not be designed to meet these needs; therefore, investments in a very limited number of military-unique systems should continue. However, given the greater overall capacity, surge capability, attractive cost, and ubiquity of commercial systems, the DoD must ascertain which military traffic can be transitioned to commercial systems. The military needs for protected communications as well as building or foliage penetration waveforms should be consolidated into a single unique MilSatCom system or incorporated into commercial systems as adjunct packages. Because a significant fraction of future military telecommunication requirements are for bidirectional CONUS to theater traffic, fiber-optics in particular offer a cost effective alternative for this large volume of traffic. While it can be argued that fiber cable is susceptible to destruction and consequently denial of service, the proliferation of redundant commercial fiber and satellite systems may make the risk acceptable for much of the traffic so long as SatCom capacity can be used as a backup for minimum essential communications.

Commercial SatCom systems, particularly a new generation of wideband data systems, could provide capacity that meets or exceeds the DoD intertheater and CONUS-to-theater unprotected wideband requirements. Two options exist for the procurement of commercial capacity. Either capacity can be leased on a system or an entire system can be procured from commercial vendors. In either approach, the costs are projected to be less than those of a DoD-designed, -acquired and -operated system. DISA initiatives for services on demand are being manifested in such ongoing programs as the Commercial Satellite Communications Initiative (CSCI) and DISN Satellite Transmission Services - Global (DSTA-G). The Task Force supports these initial efforts and encourages the DoD to build upon lessons learned to greatly expand the DoD's access to commercial, space-based communications capacity.

Commercial satellite facilities to support mobile-user military data requirements can be procured in two ways: by procuring entire commercial systems or purchasing system time. The cost data shown in Figure 65 are typical for the purchase of a commercial system. This strategy is effective if the system is used at its 2-MTW capacity. Purchasing a commercial SatCom system to support mobile users or a portion of a mobile system's capacity are options that should also be explored. For example, several of the emerging commercial LEO systems are producing large numbers of satellites, due to the sizes of the networks and the replenishment rates. Additional satellites might be procured off the production line for separate military systems; entire systems, including their maintenance and operation, could be procured from existing vendors; or communication channels could be purchased on existing commercial systems.

If time is purchased on commercial satellite systems supporting mobile users, the economics change. If time is purchased, bulk data transfer is being procured rather than a data transfer capacity. For example, if a system is owned and operated at capacity, the data transfer capacity is approximately $24/bps of capacity. If time is purchased on the system, data can be transmitted for $2–$3/Mbit. Time purchase may be appropriate for surge requirements, temporary use, or applications where full-system capacity is not needed. Long-term agreements for nonpreemptive lease or purchase of bulk data transfer should be pursued to meet surge requirements.

Internetworking these commercial systems (satellite, fiber and terrestrial wireless communications systems as envisioned in Figure 36) with one or more minimum, essential, protected DoD MilSatCom system(s) and with all other DoD telecommunication systems would provide a robust, high-capacity, flexible, and scalable DoD-wide virtual Intranet that supports warfighters' needs. This Intranet (GIG), if based on commercial Internet standards and protocols, would allow the efficient insertion, when necessary, of additional commercial telecommunication technology to meet growing needs within DoD.



The Task Force concludes that no matter how one looks at the situation, there is insufficient bandwidth to meet today's military communications needs from both the Service and Joint perspective.

Further, the Services have interoperability issues to resolve among their own systems and communications systems. The CINCs have similar interoperability problems and communication capacity shortfalls that are compounded by the need to integrate the Services' communication infrastructures.

It is the Task Force's opinion that all DoD communications acquisition over the next 10 years will not meet the anticipated (projected, but unsubstantiated) requirements. Very thorough studies of how to meet the capacity and internetting requirements must be conducted. These studies must address, in a creative manner, how the DoD can leverage commercial Internet technologies, concepts, architecture, and vision to meet DoD telecommunications requirements in the future. The Task Force notes that the private sector vision is simple, as stated earlier. However, because the way in which telecommunications systems are procured and delivered to the warfighters—numerous independent program managers acquiring technology, DoD needs to add technical depth to its vision to ensure that the many component systems can be integrated into and provide value within a DoD-wide virtual Intranet and thus value to the warfighter. In the private sector this technical depth is not necessary: market forces require that new telecommunications technology be integrated into the Internet—otherwise the technology

perishes. These market dynamics do not exist within the DoD. Consequently, a shared, detailed vision and architecture, supported by strong leadership, policies, processes, and review must be substituted until such time as the DoD-wide virtual Intranet (GIG) begins to show its value and gain momentum.

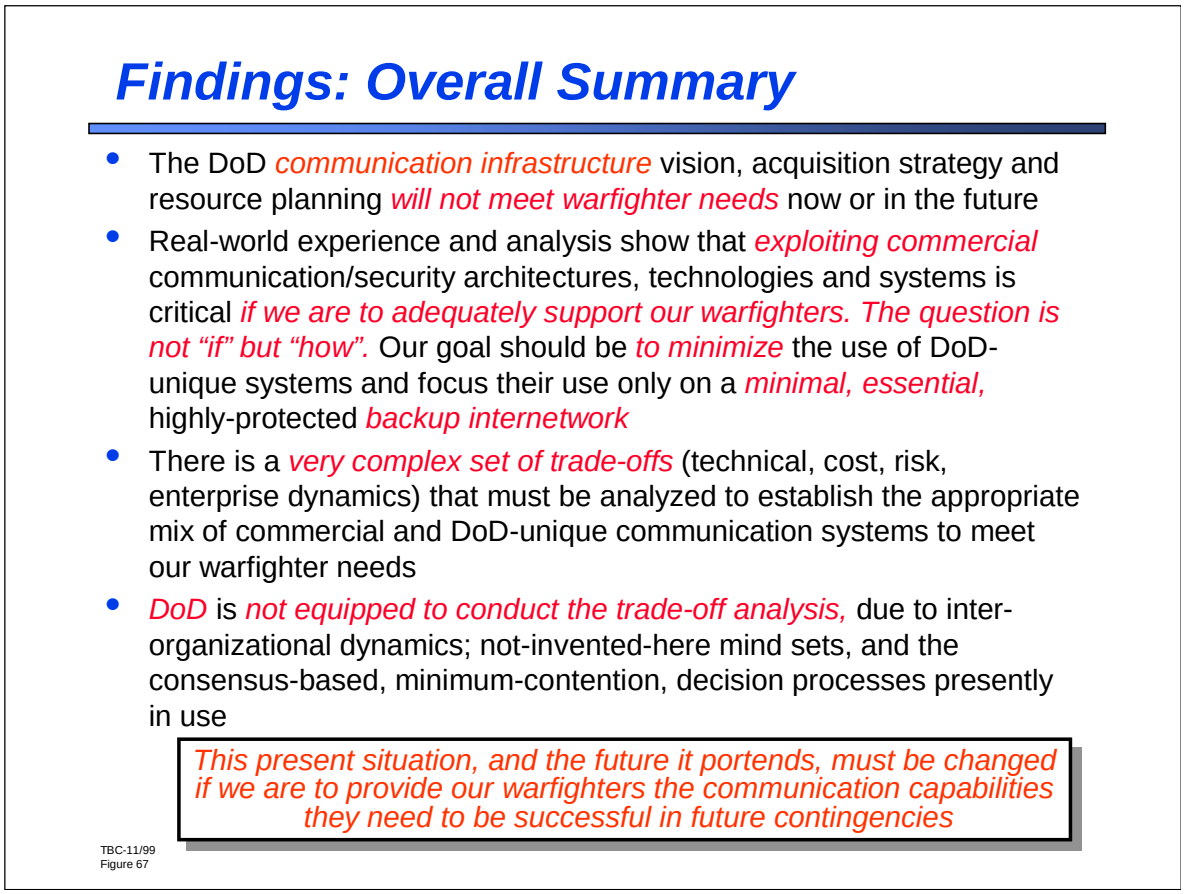
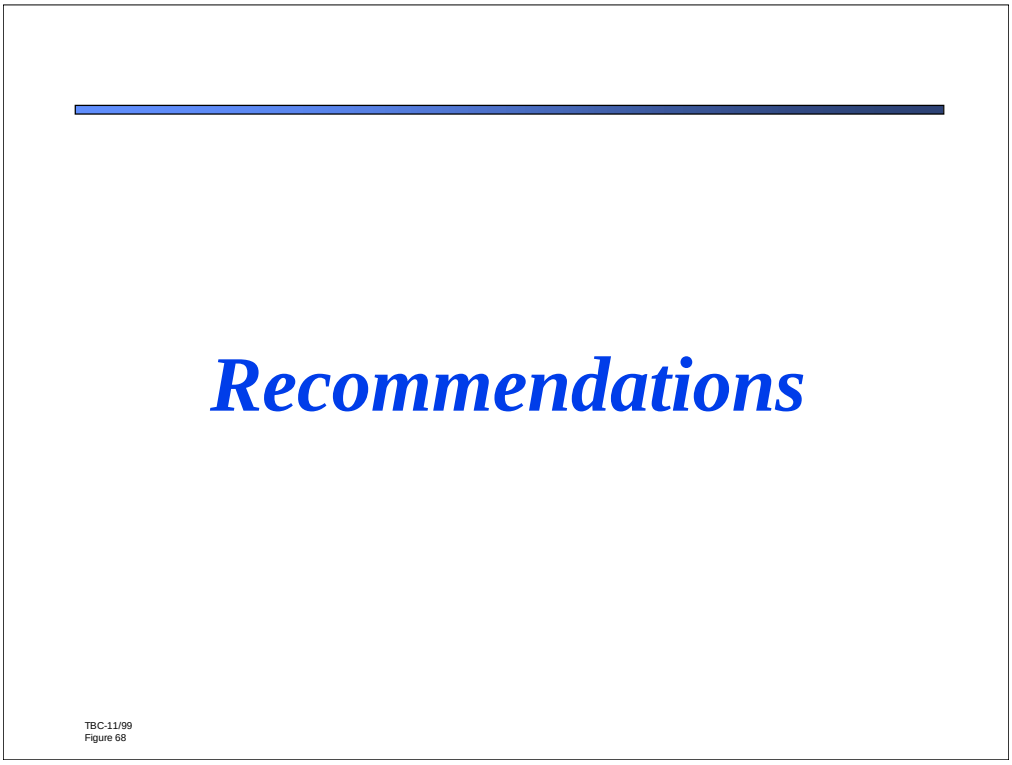
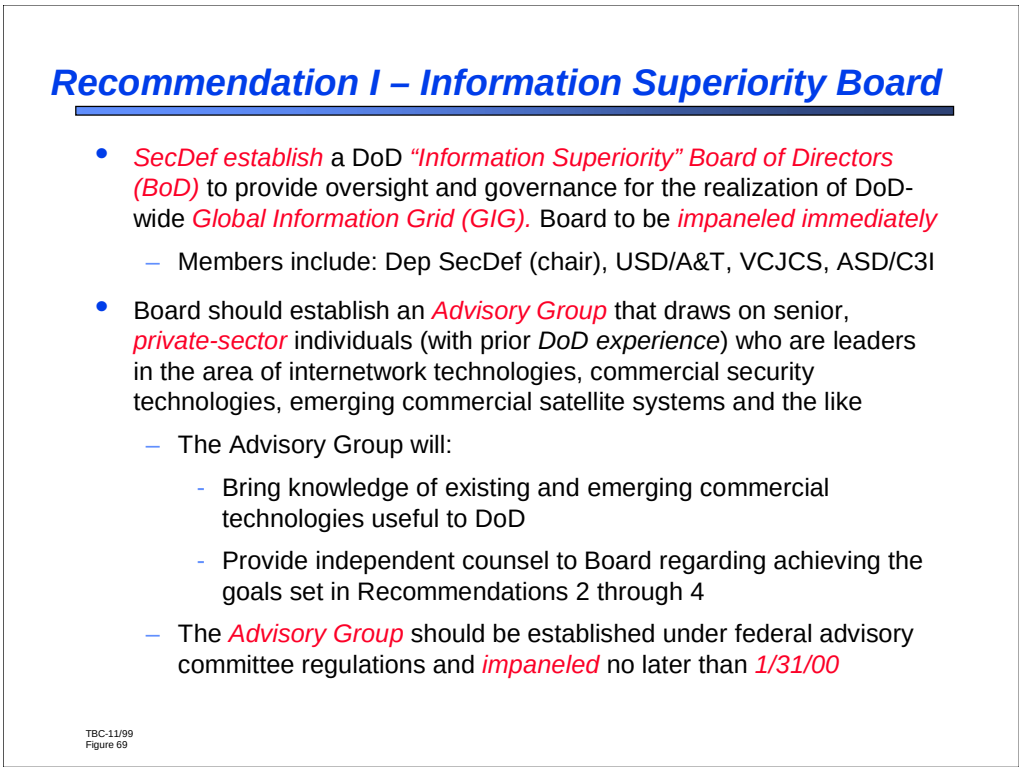


Figure 67 provides the summary findings of the DSB Task Force on Tactical Battlefield Communications. There is no question that many dedicated individuals within many DoD organizations are working hard to meet the telecommunication requirements of our warfighters. However, these activities are caught in a web of needing to meet today's needs, keeping programs funded, and satisfying multiple, diverse masters—their Services, the CINCs, and their specific organizations' missions and roles. The Task Force believes that focusing and harnessing the energy, dedication, and drive of these individuals can result in the delivery of a secure DoD-wide virtual Intranet (GIG) to meet present and future warfighter *joint* information exchange requirements. It is with this goal in mind that the Task Force offers the recommendations that are presented in the next section of this report.


Recommendations
TBC-11/99
Figure 68



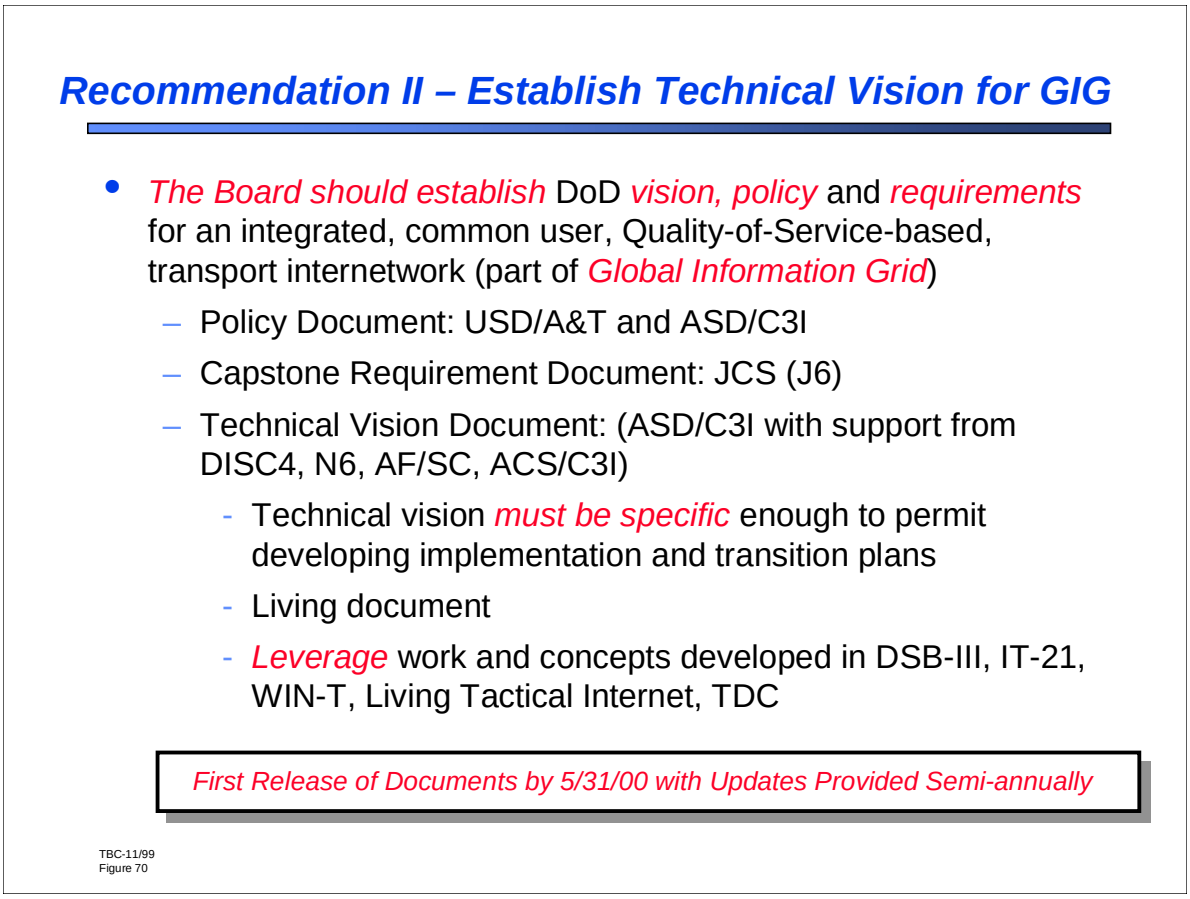
RECOMMENDATION I—INFORMATION SUPERIORITY BOARD

Consistent with its findings that under current organization, methods, and procedures the DoD is unlikely to realize a measured, consistent, and effective approach to creation of a Global Information Grid (GIG), the Task Force recommends the formation of a *DoD Board of Directors for Information Superiority*.

The Secretary of Defense should impanel the Information Superiority Board immediately, with membership consisting of the Deputy Secretary of Defense (as chair), the Undersecretary of Defense (Acquisition and Technology), the Vice-Chair of the Joint Chiefs of Staff, and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

It is further recommended that the Information Superiority Board create an Advisory Group under Federal Advisory Committee regulations (or as a permanent DSB panel) consisting of senior industry leaders. The Advisory Group's purpose is to provide the Board with up-to-date knowledge of current and emerging commercial information systems, services, and network technology of potential use to the DoD in the realization of its Global Information Grid. It is also expected to offer experience-based advice from industry as to the best technical and management methods for creating such an infrastructure.

The Advisory Group should consist of recognized industry experts in inter-networking technologies, commercial information and network security technologies, emerging information transfer technologies and systems, and other commercial activities such as standards development, infrastructure development, and the like. The Advisory Group charter should also ensure that the group provides independent assessments and counsel to the Information Superiority Board concerning the achievement of the goals and objectives set forth in Task Force Recommendations II through VI.



RECOMMENDATION II—DOD VISION FOR GIG

In briefing after briefing to the Task Force from the Services, Joint Staff, OSD, and various agencies, a circuit-centric perspective of operations and technology applications has been repeatedly reinforced. Requirements have invariably been stated only in terms of point-to-point (circuit-based) bandwidth and point-to-point circuits, without regard for the JV-2010 vision or the importance of an information and network centric environment to the conduct of future warfare.

Requirements expressed in terms of circuits clearly demonstrate a lack of understanding of the implications of the emerging packet-based networking infrastructures, and the emerging, packet-based global internetworking environment. At present, the commercial sector is moving rapidly to build, and to connect users, to a general-purpose, packet-based grid with high speed QoS-based end-to-end services. User devices such as telephones, pagers, computers, and myriad other information-age devices are already being integrated from a service-level perspective and will ultimately become integrated hardware elements of a computer-rich, seamless networking environment that is transparent to the user. Global packet-switched networks, perhaps the best example of which is the current Internet, are growing as fast as industry can produce the necessary connective devices and install the associated networking infrastructure.

The resultant of this emergent vector set is already apparent. The world will soon be immersed in an information transfer environment that enables and facilitates the free flow of information packets from object to object with little or no intervention from users or transfer providers. Every user will have the perception of being permanently and continuously "connected," regardless of location. The DoD must prepare for this eventuality in order to meet the increasingly global information needs of warriors. More specifically, the DoD must supplement its continued need to forecast point-to-point operational requirements, and point-to-point information flows at the system level, with a new emphasis on the impact of the availability and flexibility of a packet-switched GIG on operations and system architecture.

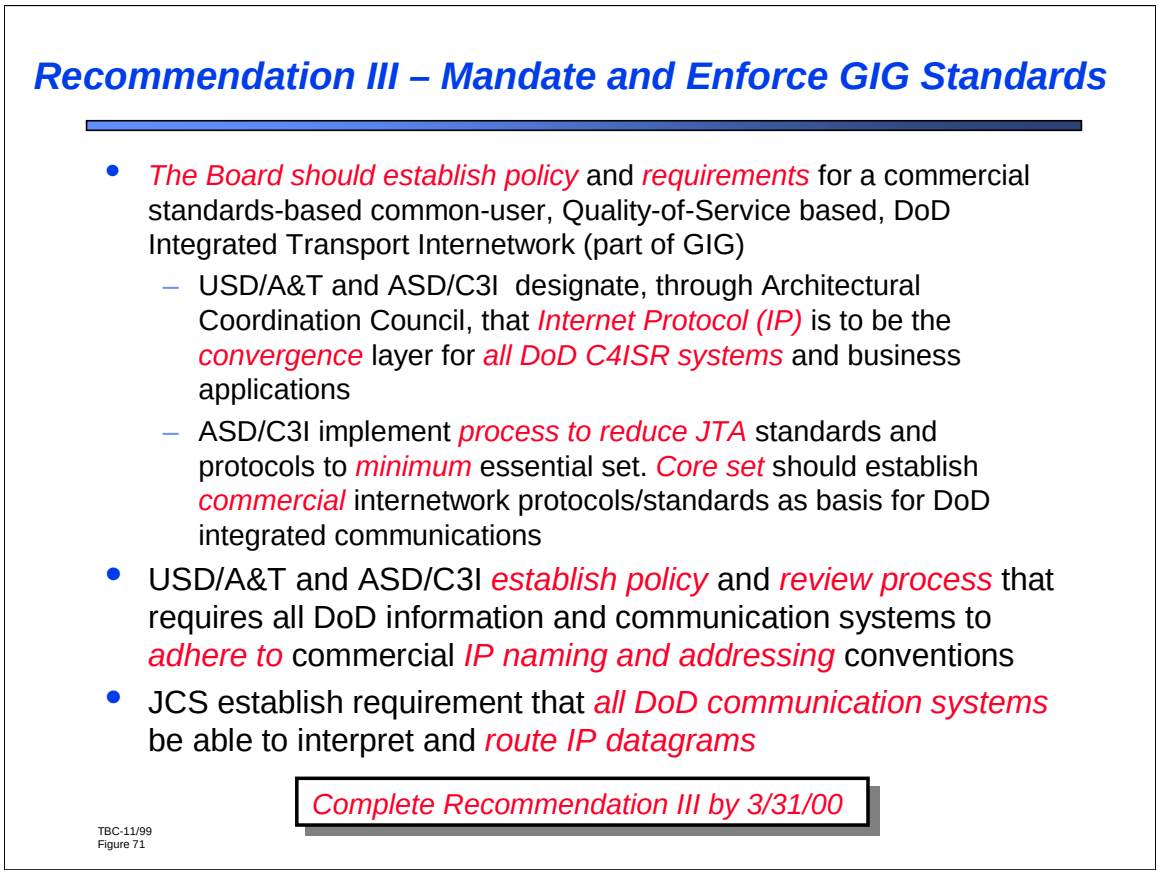
It is therefore, the recommendation of the Task Force that immediate steps be taken by the DoD to establish a detailed technical vision, supporting requirements, and policy for an integrated, common-user, QoS-based global transport network as the core of a DoD-wide virtual Intranet (GIG). The Task Force further recommends that the GIG Board of Directors direct the appropriate agencies to undertake the following activities, with the first release of the indicated documents no later than 31 May 2000 and updates provided semi-annually to reflect evolving commercial telecommunication standards and technologies.

1. The USD/T&L and ASD/C3I to develop the appropriate policy document for the GIG transport layer described above. A key area of emphasis for this document must be the implications of a quality-of-service-based GII on DoD operations, i.e., the GIG will not merely be a new communications platform for conducting business-as-usual
2. The Joint Staff, specifically the J6, to produce the capstone requirements documentation consistent with the as yet insufficiently detailed, but well-thought-out JV-2010 and Network-Centric Warfare documents. Again, a key area of emphasis must be the impact of the GIG on operations: what new operational capabilities and what new doctrine will the GIG enable?
3. The ASD/C3I to take the lead and, supported by the appropriate Joint Staff and Service elements (J6, Army DISC4, Navy N6, Air Force/SC, etc.), develop a unified technical vision document to extend JV-2010 and Network-Centric Warfare to the level of detail consistent with actual realization of these important concepts. The vision document should have the following minimal characteristics.

    a) The vision must be sufficiently specific to permit the development of implementation and transition plans by all unified Commands, Services, and DoD agencies.

    b) The vision must be a living document, consistent with reasonable expectations for advancing technology (both weapon systems and information systems) and with the expected resultant evolution in war fighting methods and organization.

    c) The vision should provide sufficient insight to DoD elements that maximum advantage can be obtained from work currently underway on such concepts and systems as DSB-III, IT-21, WIN-T, TDC, JTRS, and other DoD digital information transfer initiatives.



RECOMMENDATION III—STANDARDS-BASED GIG

Consistent with the emergent environment described in Recommendation II and elsewhere in this report, it is essential that the DoD develop the necessary policy and requirements for a commercial-standards, common-user, QoS enabled, integrated information-transfer network. Specifically, to ensure that DoD C4ISR systems are capable of interoperating with each other at the IP layer of the internetwork protocol stack, the following actions are recommended:

1. A commercial-standards-based common-user, QoS-enabled integrated information transfer internetwork, as prescribed in Recommendation II requires that ASD/C3I and USD/AT&L designate, through the Architectural Coordination Council, IP as the convergence layer for all DoD information systems.
2. A process must be developed and implemented to reduce Joint Technical Architecture (JTA) standards and protocols to the minimum essential set. The core set of directives for the DoD integrated information transfer system must call out commercial inter-network protocols and standards. The goal of the JTA is to promote C4ISR interoperability through the use, by DoD, of the smallest possible number of commercial interface standards, protocols, and commercially-supported software components, NOT to be a compendium of (non-interoperable) commercial and military standards.

3. ASD/C3I and USD/AT&L establish a policy and a review process that requires all DoD information and communication systems to adhere to commercial IP naming and addressing conventions. This is essential for DoD to easily, efficiently, and cost effectively leverage commercial IP-based products and services.
4. The Joint Staff establish a requirement that all DoD communication systems be able to interpret and route IP datagrams, so that DoD systems can be integrated into a single internetwork that can in turn link to and integrate seamlessly with commercial networks.

Recommendation IV – Implementing the GIG

- *The Board should establish an Executive Office* responsible for *leading* and *implementing* the DoD-wide, common-user internetwork (transport component of GIG)
  - *Executive Director* should be a minimum *five year appointment* and *tasked* to develop an *implementation plan and processes,* including technical milestones, measurable interim goals and identify resources to permit *completion of GIG by 9/30/03*
  - *The Board should provide system engineering resources* to the Executive Office through a dedicated system engineering team comprising *20 to 30 outstanding* network *systems engineers* drawn from throughout DoD

Office and Leadership Position Established by 2/29/00

Systems Engineering Office and Billets set up by 2/29/00

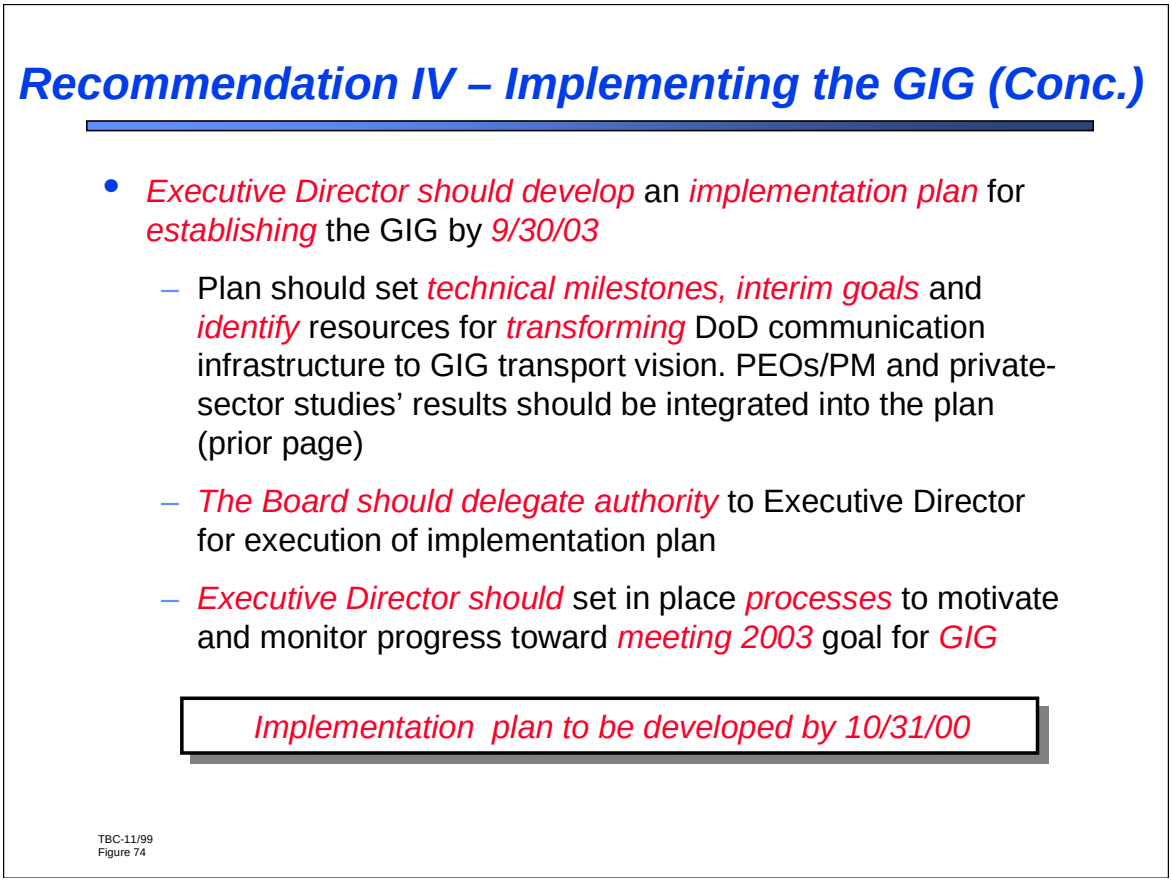
TBC-11/99
Figure 72

Recommendation IV – Implementing the GIG

- *Executive Director should establish processes to transform DoD communications* from a circuit/broadcast centric framework to a common-user internetwork framework based, to the maximum extent possible, on commercial standards, protocols and technologies
- *Executive Director should,* with ASD/C3I and USD/A&T support, *task* all DoD and *Service PMs/PEOs* responsible for tactical/strategic communication systems to:
  - *Conduct studies* on how *to transition their system,* by the end of next POM cycle, to permit integration into common DoD internetwork. Study should identify technical challenges, cost and schedule for transition
- *Executive Director should fund two competitive* industry *studies* that address *how* (not if) emerging *commercial communication* satellite systems, fiber infrastructure and mobile internetwork technologies *can be exploited* to implement a DoD-wide internetwork. Estimated cost $2M each

Complete All Studies by 7/31/00

TBC-11/99
Figure 73



RECOMMENDATION IV—GIG IMPLEMENTATION PROCESS

Placing the proper emphasis on GIG implementation and ensuring adherence to the policies established in accordance with the previous recommendations requires continuous oversight. It is therefore recommended that the Board of Directors for Information Superiority create, by 29 February 2000, an Executive Office responsible for leading the implementation of the DoD-wide common user internetwork on behalf of the Board. The Executive Office Director should be a senior DoD leader appointed for a minimum of five years.

Several additional, more specific actions are needed to accomplish the GIG objectives:

1. The Executive Director should be tasked to develop a GIG implementation plan, to include technical milestones, measurable interim goals, and an estimate of the resources necessary to complete transition and realization of the GIG by 30 September 2003.
2. The Board of Directors should provide manpower billets for a system engineering team to support the Executive Director. A cadre of 20 to 30 outstanding system engineers with backgrounds in Internet telecommunications and security technologies should be selected from throughout DoD. These individuals must be deep technically and visionary in their system engineering skills. This system

engineering team would provide independent technical inputs to the Executive Director regarding the many responsibilities this individual will be given as noted in paragraphs 3 to 5 that follow.

3. The Executive Director should immediately establish a process to transform DoD communications from the present circuit and broadcast-centric framework into a global DoD-wide common-user virtual intranet. This transformation must embody the current and evolving commercial standards, protocols, and technology, with the goal of reducing inefficiency in spectrum usage and the costs associated with inefficient dedicated DoD services (circuits). Most important, this transition should enable new operational flexibility that can be leveraged by warfighters.

4. USD /AT&L and ASD/C3I should task all DoD and Military Services Program Managers/Program Executive Officers responsible for tactical or strategic communication systems to conduct studies on how to transition their respective systems to a state such that they can be readily integrated into the common DoD internetwork. Such studies should identify technical challenges, costs, and schedules of the said transition.

5. The Executive Director should fund two competitive industry studies that independently address how (not whether) the emerging commercial communication satellite systems, fiber infrastructure, and mobile inter-networking technologies can be exploited to implement the GIG described here. The Task Force estimates the cost of each such study at $2 Million, and recommends the completion of this work not later than 31 July 2000.

Recommendation V – GIG Security

- OSD and Service *CIOs,* under OSD leadership, should
  - *Set* security *policies* and *procedures* that:
    - Establish sense of *urgency* regarding information security
    - Hold Commanders *accountable* (strategic, operational, tactical)
    - Establish *education* and *training* procedures for all DoD personnel
    - Establish *red-team* testing and crisis action response teams
    - Require test, evaluate, fix — test, evaluate, fix —
  - *Leverage commercial practices, technologies* and *investments* such as:
    - *Emerging* standards-based security *architecture* (CDSA)
    - Applications and network level *security products*
    - *Emerging practices* for:
      - *Defense-in-depth*
      - *Risk management*
      - *End-to-end security*
      - Defense against the *insider threat*

TBC-11/99
Figure 75

Recommendation V – GIG Security (Conc.)

- *Formulate/execute* a "balanced mix" *security strategy, architecture and policies for the GIG* that:
  - *Uses evaluated commercial* security *framework* and *technologies*
  - *Augments commercial* technology *only as necessary* to meet unique DoD needs
  - *Influences* commercial technology *through strategic partnerships*
  - Addresses the "not-invented-here" mindset

Have strategy, policy, architecture and procedures in place by 8/30/00

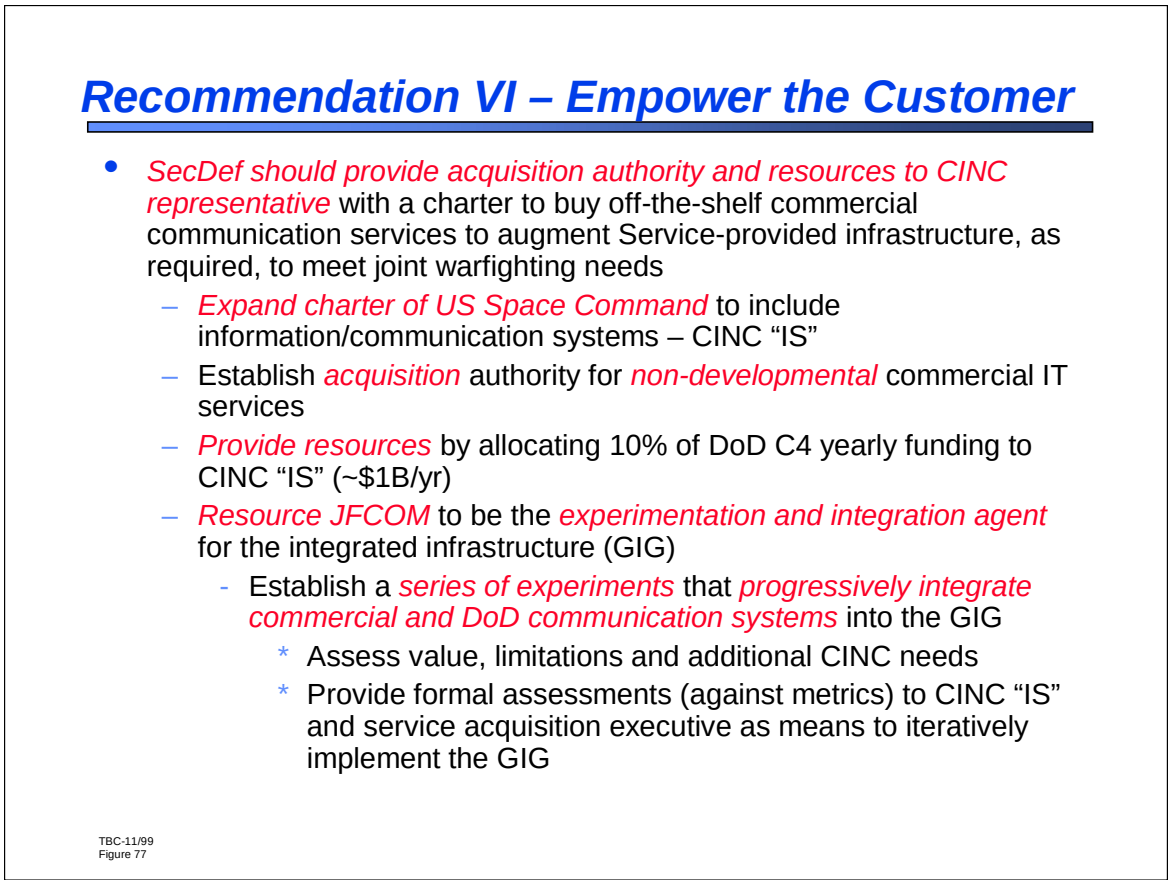
TBC-11/99
Figure 76

RECOMMENDATION V—GIG INFORMATION SECURITY

In response to the findings related to the protection of DoD information and information systems, the Task Force recommends the following actions be undertaken by OSD and Service CIOs under OSD leadership:

1. Establish security policies and procedures that
    a) Create a sense of urgency regarding information security
    b) Hold commanders (strategic, tactical, and operational) accountable
    c) Create and apply effective and continuous information protection education and training for all DoD personnel
    d) Create red-team testing and crisis action response teams, standardized across the DoD.
    e) Require continuous "test, evaluate, fix" actions among all DoD agencies and the military services.
2. Seek to obtain maximum leverage from commercial practices, technologies, and investment in Internet information security, particularly with respect to
    a) Policy, management, and application of information and information systems security
    b) Emerging standards-based security architecture (e.g., Common Data Security Architecture [CDSA])
    c) Applications and network level security products (e.g., Public Key Infrastructure, IPSec, SSL, PGP, S-SNMP, SMIME, Virtual Private Networks, and the like)
    d) Emerging practices for
        1) Privacy, authentication, integrity, continuity of service, verification and nonrepudiation
        2) Defense in depth
        3) Risk management
        4) End-to-end security
        5) Defense against insider threats.
3. Formulate and execute a balanced mix security strategy and architecture for the GIG that
    a) Employs evaluated commercial security practices and technologies
    b) Augments commercial technology only as necessary to satisfy truly unique DoD needs
    c) Influences commercial technology through strategic partnering
    d) Addresses the currently prevalent "not invented here" mind-set.

The security strategy, architecture policies and procedures for the GIG should be in place by 30 August 2000 and reviewed annually as the GIG comes into being.



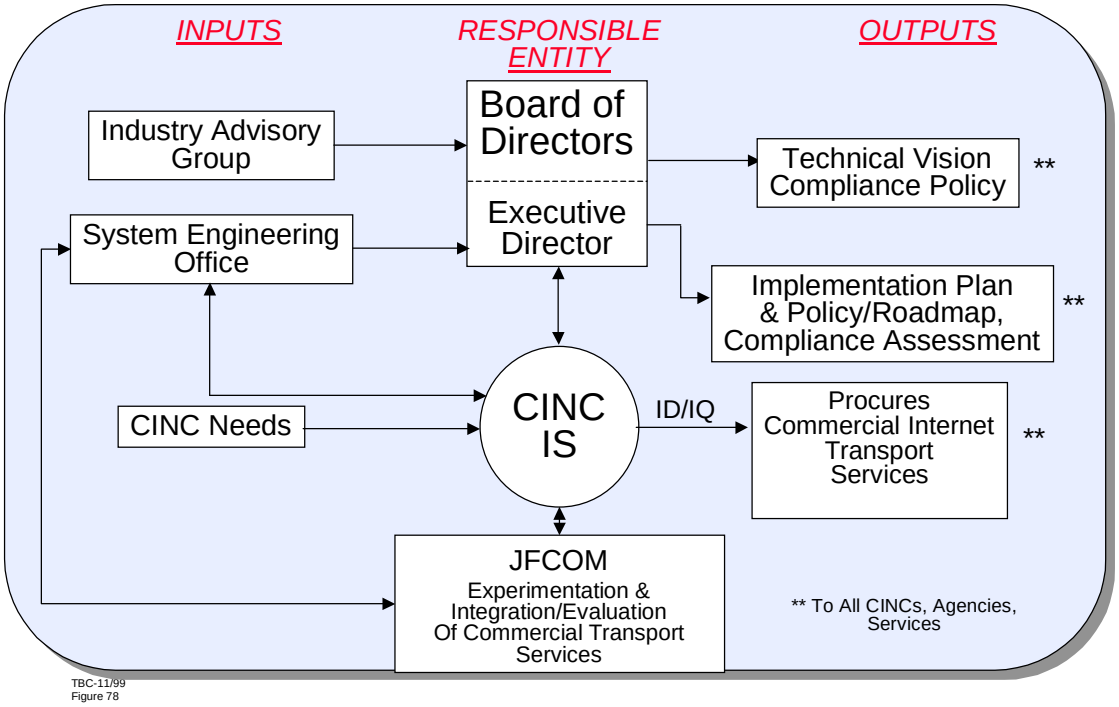
RECOMMENDATION VI—EMPOWER THE CUSTOMER

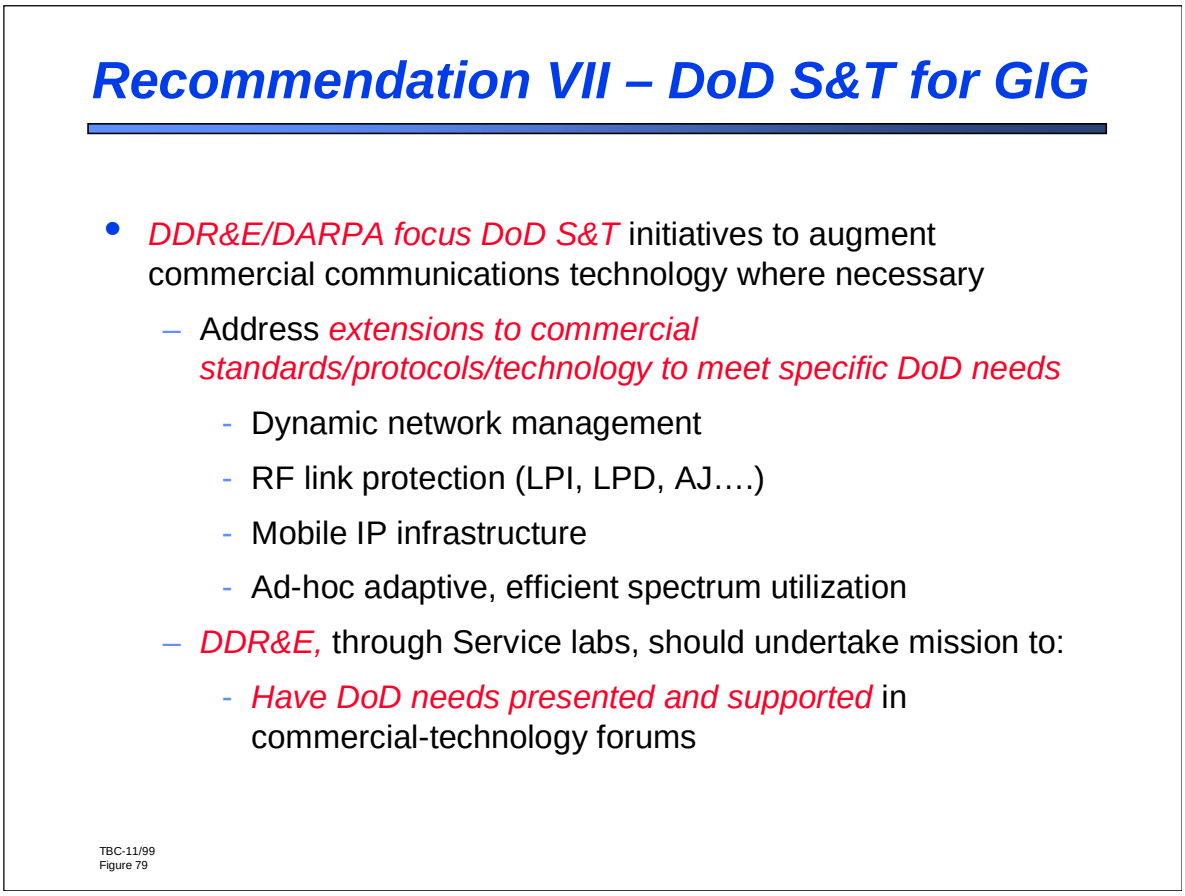
It is essential that the DoD create a mechanism to expedite the use of rapidly evolving commercial information technology to meet the needs of DoD customers. This recommendation represents a major change in the traditional approaches regarding the acquisition of information technology, and requires an alternative acquisition process for the CINCs, in order to encourage and reward customer-driven and innovative acquisition practices and behaviors throughout the Department. The Task Force therefore recommends that the Secretary of Defense provide acquisition authority to a selected CINC, with an attendant charter to buy off-the-shelf commercial information and services to augment the Service-provided infrastructure, as required, to meet joint warfighting needs. In particular, the Task Force recommends the following.

1. Expand the charter of USCINCSPACE to include information and communication systems, thus establishing a supporting CINC for Information Systems (CINC IS)
2. Establish acquisition authority for USCINCSPACE for nondevelopmental commercial IT services
3. Provide resources by allocating 10% of DoD annual C3 funding to USCINCSPACE (approximately $1 Billion/year)

4. Expand the charter and resources of CINCUSJFCOM to include responsibility as test and evaluation agent for the DoD global information infrastructure. Joint Forces Command (JFCOM) should also establish a series of experiments that progressively integrate commercial and DoD communication systems into the GIG, and additionally
    a) Assess the value, limitations, and performance of such integrated systems against current and emerging CINC requirements
    b) Provide resultant formal assessments (against established metrics) to USCINCSPACE and Service acquisition executives as a means to iteratively implement the GIG.

Recommendations I through VI – Policy & Guidance Structure



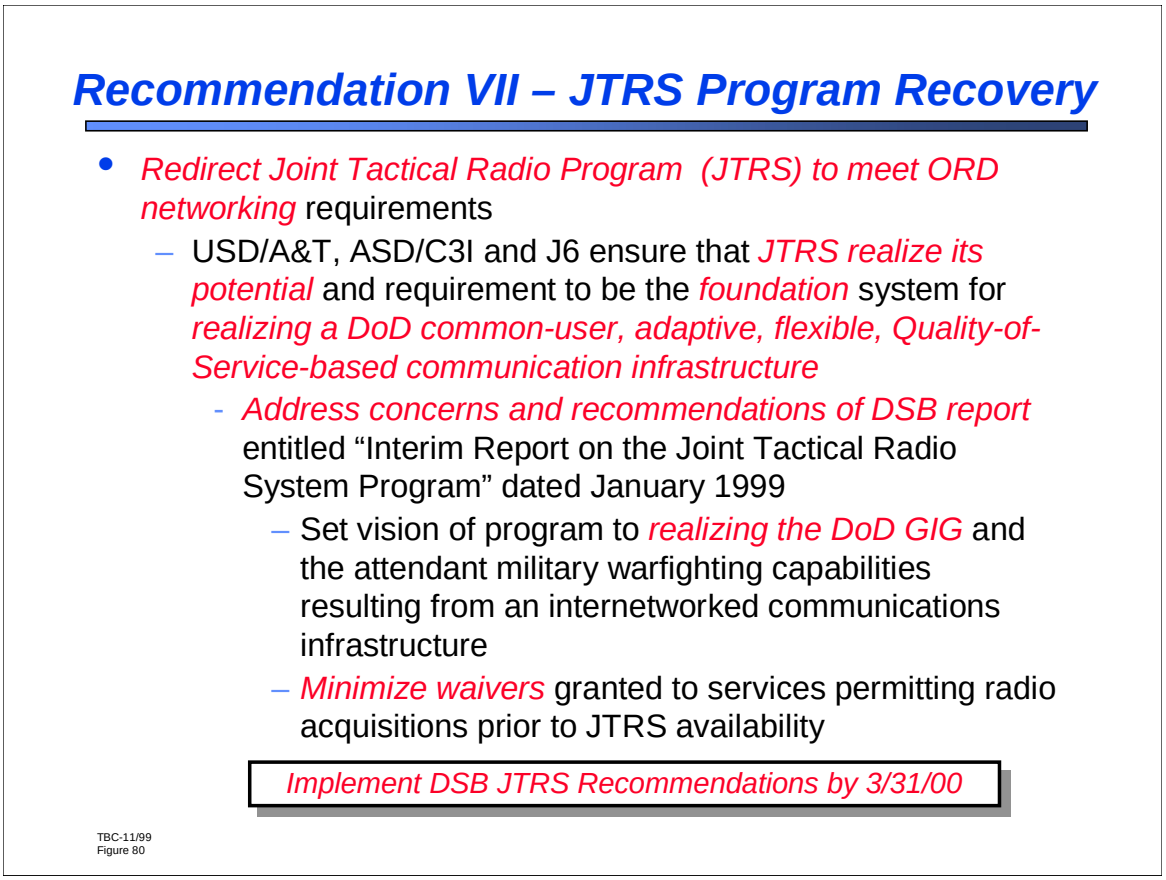


RECOMMENDATION VII—DOD S&T FOR THE GIG

Consistent with the previous recommendations, it is essential to provide a DoD Science and Technology strategy that focuses S&T initiatives to augment commercial technology where that proves necessary for special DoD needs. Specifically, the Task Force recommends that

1. DDR&E and DARPA address extensions to commercial standards, protocols, and technology to meet such specific DoD needs such as
   a) Dynamic network management
   b) RF link protection such as low probability of detection/intercept (LPI/LPD)
   c) Provision of a robust, mobile-IP infrastructure
   d) Establishing efficient, ad hoc, adaptive spectrum utilization procedures and services.

Furthermore, DDR&E, through the Service laboratories, should undertake a task to ensure that DoD needs are presented and supported in commercial information technology and standards forums.



RECOMMENDATION VIII—JTRS PROGRAM RECOVERY

The Task Force has repeatedly expressed its concern to the DoD about shortfalls in the Joint Tactical Radio System program with respect to the emerging and rapidly expanding digital, mobile, ad hoc networking environment in the private sector. At present, the JTRS program is defined as, and limited to, providing successor capabilities to replace aging radio equipment and accommodate traditional waveforms in use throughout the DoD. This role is far too limited for today's powerful digital programmable wireless capabilities. Furthermore, the DoD is substantially overlooking the major information-system integration potential in this new technology. (See the DSB Tactical Battlefield Communications Task Force *Interim Report on the Joint Tactical Radio System*, dated January 1999, in Annex D of this report).

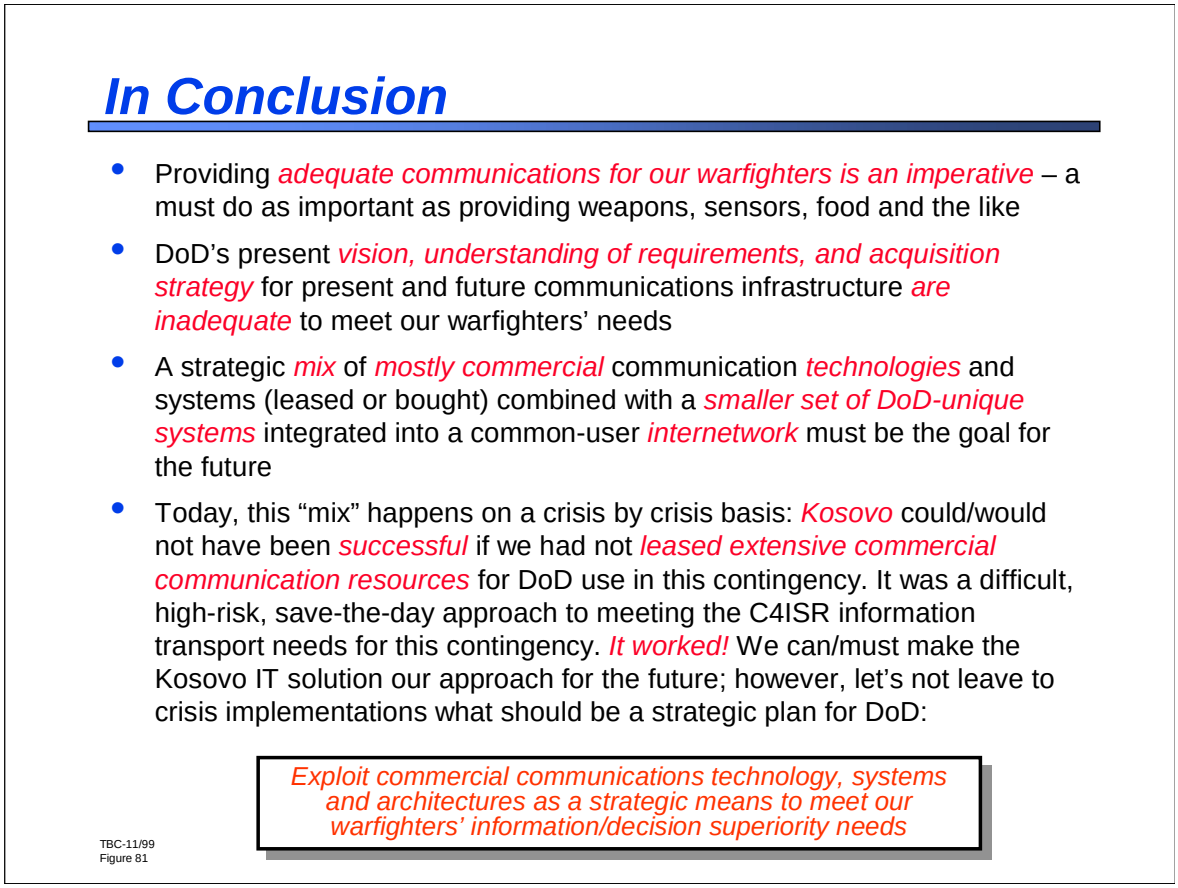
For the reasons stated previously, the Task Force again recommends that the JTRS program be redirected to address Joint Operational Requirements Document (ORD) networking requirements. USD/AT&L, ASD/C3I, and Joint Staff/J6 are urged to ensure that the JTRS program be reformulated to realize the potential of the JTRS as the foundation for the ground component of a DoD common user, adaptive, flexible, QoS-based transport layer for its Global Information Grid. Immediate redirection to the JTRS program should be given to the following:

1. Set forth a vision for the program related to focusing on, and providing universal networking bridging services that will enable warfighters to interface

and interoperate with other information transfer media on demand and create ad hoc internetworks as needed

2. Accelerate the JTRS acquisition and minimize waivers given to the Services that allow other radio acquisitions prior to JTRS availability.

5 CONCLUSION



Providing adequate telecommunications to our warfighters is an imperative—a must-do as important as providing weapons, sensors, food, and the like. DoD's present vision, understanding of requirements, and acquisition strategy for present and future communications infrastructure are inadequate to meet our warfighters' needs. A strategic mix of mostly commercial telecommunication technologies and systems (leased or bought), combined with a smaller subset of DoD-unique systems integrated into a common-user DoD-wide virtual Intranet must be the goal for the future.

Today, this mix of technologies happens on a crisis-by-crisis basis: the operation in Kosovo would not have been successful if we had not procured, in real time, extensive commercial telecommunication services for DoD use in this contingency. This difficult, high-risk, save-the-day approach to meeting the C4ISR information transport needs for this contingency worked! We can and must make the Kosovo exploitation of commercial telecommunication systems and technology the cornerstone of our approach for the future. Let us not leave to crisis implementation what should be a strategic plan for DoD. Building the DoD GIG on this strategy must proceed immediately.

ANNEX A

TERMS OF REFERENCE

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-3010

ACQUISITION AND
TECHNOLOGY

DEC 2 9 1998

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference--Defense Science Board Task Force on Tactical Battlefield Communications

You are requested to form a Defense Science Board (DSB) task Force on Tactical Battlefield Communications to determine U.S. needs for wireless communications on future battlefields and the adequacy of communication architecture plans to fulfill those needs. You should specifically address the ability of digital and analog communications below the Corps-level to support predicted demands of joint tactical, intelligence, logistics and medical actions while assuring combatants' effectiveness and safety.

Tasks to be Accomplished:

The Tactical Battlefield Communications Task Force will provide advice, recommendations, and supporting rationale that address the items below for OSD, the Military Departments, the Joint Staff, Unified and Specified Combat Commands and the Defense Agencies:

-- Adequacy of forecasted tactical communications requirements for evolving concepts such as Army After 2010, Operational Maneuver from the Sea, Air Expeditionary Force and Extended Littoral Battlespace. Interoperability requirements to support joint operations, should also be reviewed.

-- Adequacy of DoD communication vision and architectures capable of meeting forecasted service and joint requirements.

-- Adequacy of companion communication security architecture to assure force protection and information assurance.

-- Funding and capitalization constraints that restrict ability to make the transition from equipment in the current inventory to equipment needed to meet the evolving communications requirements.

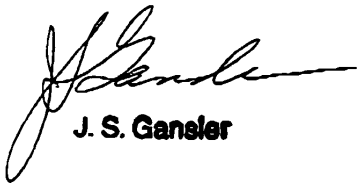
-- Adequacy of tactical communications equipment now in the DoD inventory, or under development, to fulfill the evolving communications requirements, to include; operational experience with communications equipment in ATDs and ACTDs.

-- Adequacy of acquisition strategy and policy to meet evolving communication architectures and requirements that facilitates exploiting of commercial and DoD-developed technologies and services.

The Task Force should provide specific advice for addressing its findings.

The study will be co-sponsored by the Under Secretary of Defense (Acquisition and Technology), the Senior Civilian Official, OASD (C3I) and the Director, JCS(J-6). Dr. Michael Frankel will serve as the Task Force Chairman. Mr. Bennett Hart, OASD/C3I, will serve as the Executive Secretary and Maj Tony Yang, USAF, will serve as the Defense Science Board Secretariat Representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5104.5, "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.



J. S. Gansler

ANNEX C

AGENDAS

AGENDA

DSB Task Force on Tactical Battlefield Communications

19 November 1998

Time	
7:30	Coffee/Tea
8:00	PDUSD(A&T) Comments—Honorable Dave Oliver (Invited)
8:30	General Counsel Briefing—Mr. David Ream
8:45	Chairman's Opening Remarks—Dr. Mike Frankel
9:15	Study Plan—Dr. Mike Frankel
9:45	Break
	OSD Perspective
10:00	Joint Tactical Radio System (JTRS) Background/History
	Mr. Vic Russell, OASD(C3I
10:15	Joint Requirements /Army Requirements
	Col James Schroeder, Army TRADOC Systems Manager
11:30	Program Overview and Status
	Col Tony Badolato, JTRS Program Manager
12:00	Lunch
Services Perspectives—Existing programs and proposed JTRS Migration Plans	
12:30	Navy requirements
	CAPT Gary Graupmann, Navy PM DMR
1:30	Air Force Requirements
	Briefers TBD, POC is Col Bobby Smart,
2:30	Break
2:45	Marine Corp Requirements
	Col Robert Logan, Director Requirements Division, Combat Development Command. POC is Maj Herb Bowlds,
3:45	Discussion
5:00	Adjourn

AGENDA

20 November 1998

Private Sector Perspectives (open standards, line level vs. box competition, etc.)

Time	
7:30	Coffee/Tea
8:00	Motorola – DMR—Mr. Mike Lyga
9:00	ITT – NTDR—Mr. Ed Dauksz,
10:00	Break
10:15	Raytheon – DMR, JTT, AITG—Bill Langford
11:15	Rockwell – ARC-210/DCS-2000—Mr. Ken Kato
12:15	Lunch
12:45	Open Standards Briefing—Col Mick Hanratty
2:00	Member Discussions—Members and Advisors
3:30	Adjourn

AGENDA

DSB Task Force on Tactical Battlefield Communication

Session Goal: Determine adequacy of forecasted tactical communication requirements for evolving concepts such as Army 2010, Operational Maneuver for the Sea, Air Expeditionary Forces, and Extended Littoral Battlespace. Interoperability requirements to support joint operations should also be reviewed.

11 January 1999

TIME	
7:30	Coffee/Tea
8:00	Task Force General Discussion (Mr. Arthur Money)
9:00	Army – Army 2010 Communications Requirements (Col. John Deal)
9:50	BREAK
10:00	Navy – Operational Maneuver From Sea Communications Requirements (Capt. Renny Ide)
11:00	Air Force – Expeditionary Force Communication Requirements. (Maj. Woody Wood)
12:00	LUNCH
12:30	USMC – Extended Littoral Battlespace (Col. Bob Logan)
1:30	DOD – Informational Interoperability and Architectures (Mr. Jack Zavin)
3:15	BREAK
3:30	Operational Requirements–Joint Vision (Mr. Garstka)
4:30	Task Force General Discussion (Members/Advisors Only)
5:00	ADJOURN

AGENDA

12 January 1999

TIME	
7:30	Task Force Informal Discussion (Coffee/Tea)
8:30	EUCOM Requirements (LtCol Robert Steele via VTC)
9:00	ACOM Requirements
10:00	BREAK
10:15	CENTCOM Requirements (COL Culbert via VTC)
10:45	STRATCOM Requirements (Mr. Robert Fisher)
11:15	SPACECOM Requirements
12:00	LUNCH
1:00	SOUTHCOM Requirements
1:30	TRANSCOM Requirements
2:00	PACOM Requirements (Maj David Pierce via VTC)
2:30	SOCOM Requirements
3:00	BREAK
3:15	Task Force Group Discussion (Members/Advisors Only)
4:30	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

1100 North Glebe Road, 11th Floor, Arlington, VA

Session Goal: Adequacy of DOD Communication Vision and Architecture capable of meeting forecasted services and joint requirements

18 February 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Army Communication Requirements (COL John Deal)
9:30	NETWARS Modeling and Simulation (Lt Col Pat Vye)
10:30	BREAK
10:45	RAND Study on Information Infrastructure (Mr. Tim Bonds)
12:00	LUNCH
12:30	GLOBAL GRID (Mr. Lee Hammarstrom)
1:30	Task Force Discussion
2:30	INFOSPHERE (Lt Gen Donahue)
3:30	BREAK
3:45	Task Force Discussion
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication
1100 North Glebe Road, 11th Floor, Arlington, VA
19 February 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Motorola: The system and corporate vision for the future (Mr. Bill Harding)
9:30	Iridium: The system and vision for the future (Mr. Bill Harding)
10:30	BREAK
10:45	TELEDESIC: The system and corporate vision for the future (Mr. Dell Williams, CEO)
12:00	LUNCH
12:30	UUNET*: Vision for the future of their Information Infrastructure (Mr. Mike O'Dell)
1:30	SPRINT*: EarthLink vision for the future of Information Infrastructure (Mr. Jim Pearce)
2:30	Task Force Discussion
3:30	ADJOURN

* The question of how they plan/design to upgrade their infrastructure with minimum disruption

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Randolph Street, Arlington, VA

Session Goal: Adequacy of DOD Communication Vision and Architecture capable of meeting forecasted services and joint requirements. Adequacy of communication security architecture to assure protection and information assurance

18 March 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	
9:45	BREAK
10:00	INFOSPHERE —LtGen Donahue
11:30	Sensor to Shooter Communications Interoperability
	CAPT Steve Soules (USN) Director, Decision Support Center
12:30	LUNCH
1:30	Laurette Bradley (Director of computing Infrastructure and standards at GTE)
2:30	Army After Next (Col Dan Bourgoine (TRADOC) & LTC Pat Nichols)
3:30	BREAK
3:45	Task Force General discussion
4:45	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Randolph Street, Arlington, VA

19 March 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Navy IT-21 (RADM John Gauss)
9:45	BREAK
10:00	LORAL (Chief Engineer Chris Hoburce & Ray Barker)
11:00	
12:00	LUNCH
12:30	
1:30	
2:30	Task Force Discussion
3:30	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Drive, Arlington, VA

Session Goal: Task Forces members presenting findings and conclusions.

22 April 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Mr. Owen Wormser (Findings to Date)
9:00	Professor Gary Minden (Findings to Date)
9:30	Dr. William Evers (Findings to Date)
10:00	BREAK (Task Force Discussion)
10:15	Dr. Scott Snyder (Findings to Date)
10:45	Mr. Peter Steensma (Findings to Date)
11:15	Dr. Reza Eftekari (Findings to Date)
11:45	Gen Carl O'Berry (Findings to Date)
12:15	LUNCH
1:00	Mr. John Stenbit (Findings to Date)
1:30	Mr. Mark Rich (Findings to Date)
2:00	Mr. Vic Russell (Findings to Date)
2:30	Mr. David Keetley (Findings to Date)
3:00	BREAK
3:15	Professor Stu Personick (Findings to Date)
3:45	Task Force Discussion
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Drive, Arlington, VA

Session Goal: Security and Systems

23 April 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Motorola, Mr. Mike Lyga (Tactical Data Communications)
9:30	Harris, Mr. Emil Svatik (Phased Array Antenna)
10:30	BREAK
10:45	Cylink, Mr. Charles Williams
12:00	Lunch:
1:00	Boeing, Mr. Jim Freeman (Phased Array Antenna)
2:00	DISA, Mr. Steven Weyman (Communications and C2 Directorate)
3:00	Task Force Discussion
3:30	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Drive, Arlington, VA

20 May 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Last Tactical Mile FEA Final Results (Mr. Bennett Hart, OASD,C3I)
10:00	BREAK
10:15	ICNIA (Mr. Joe Gerard, TRW)
11:15	Task Force discussion (Dr. Mike Frankel)
12:30	LUNCH
1:00	DoD Satellite Architecture Overview (Col Ed Alexander, OASD,C3I)
2:30	Airborne Comm Node "ACN" (Mr. Kirk Brandt, DARPA)
3:30	DoD Spectrum/Frequency (Ms. Cindy Raiford, C3I)
4:30	Task Force Discussion
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Drive, Arlington, VA

21 May 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	CMA Mix Study Brief (Dr. Steve Huffman, MITRE)
10:00	BREAK
10:15	WIN-T (Col Edward Siomacco, Army)
12:00	Working Lunch with Airborne Comm Node "ACN" (Mr. Kirk Brandt, DARPA)
1:00	Views on Battlefield Tac Comm needs and LTM Problem (Mark McHenry, DARPA)
3:00	Task Force Discussion
3:30	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Drive, Arlington, VA

24 June 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Our Vision, TEAM 2 (Carl, Mike)
9:30	Global Information Grid (Lt Col Risher, USAF)
10:00	BREAK
10:45	Global Grid Architecture (Mr. Len Schiavone, MITRE)
12:15	LUNCH
1:00	Requirements, TEAM 1 (Reza, Bill, Gary)
1:45	Spaced Based Comms TEAM 3 (Mark, Reza, Peter, John)
2:30	GNIE (John Osterholz)
3:30	BREAK
3:45	Security TEAM 4 (Owen)
4:30	Task Force Discussion
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Drive, Arlington, VA

25 June 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	CEC (Capt. Dan Busch)
9:30	Fiber Technology TEAM 5 (Gary)
10:30	BREAK
10:45	Unisys (LTG Bob Myer USA(Ret) and Mr. Frank Creaser)
12:00	LUNCH
1:00	Ownership Costs TEAM 6 (Vic)
2:00	ANA/MUOS (Richard Mendez)**
3:00	Task Force Discussion
3:30	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Drive, Arlington, VA

Session Goal: Network Security

22 July 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	JTRS (Col. Tony Badolato)
9:30	Xerox (John Lambeth, CIT)
10:30	BREAK
10:45	Cisco (Robert Deutsch, Network Security)
12:00	LUNCH
1:00	Verisign (Nick Piazzola, Commercial Security Technology)
2:00	Quantum Computing (Keith Miller, NSA)
3:00	BREAK
3:15	Federal Reserve Board (Mariane Emerson, Deputy Director IT and Security)
4:15	Task Force Discussion
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Drive, Arlington, VA

Session Goal: Network Security

23 July 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	The Open Group (CDSA, Joe Bergmann)
9:30	Task Force Discussion
10:30	BREAK
10:45	Task Force Discussion
12:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

Arnold and Mabel Beckman Center, Irvine California

Session Goal: preparing out brief

5 August 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Review of final report
10:30	BREAK
10:45	Review of final report
12:00	LUNCH
1:00	Review of final report's recommendations
3:00	BREAK
3:15	Review of final report's recommendations
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

Arnold and Mabel Beckman Center, Irvine California

Session Goal: preparing out brief

6 August 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Rework final report's slides and recommendations
10:30	BREAK
10:45	Rework final report's slides and recommendations
12:00	LUNCH
1:00	Rework final report's slides and recommendations
3:00	BREAK
3:15	Rework final report's slides and recommendations
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Dr. Arlington, Va.

9 September 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Task Force Discussion on Final Report
9:30	Acquisition Reform, success and future forecast. (Mr. Richard Sylvester OUSD/AT)
10:45	BREAK
11:00	DREN Overview, (Mr. Don Endicott, SPAWAR U.S. NAVY)
12:15	LUNCH
1:00	Task Force Discussion on Final Report
3:00	BREAK
3:15	Task Force Discussion on Final Report
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Dr. Arlington, Va.

10 September 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Task Force Discussion on Final Report
9:30	DT&E Overview, (Mr. Fred Myers)
10:30	Acquisition Reform, success and future forecast. (Mr. Richard Sylvester OUSD/AT)
12:00	LUNCH
1:00	Task Force Discussion on Final Report
3:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Dr. Arlington, Va.

7 October 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Task Force Discussion on Final Report and Out Brief Slides
10:45	BREAK
11:00	Task Force Discussion on Final Report and Out Brief Slides
12:15	LUNCH
1:00	Task Force Discussion on Final Report and Out Brief Slides
3:00	BREAK
3:15	Task Force Discussion on Final Report and Out Brief Slides
5:00	ADJOURN

AGENDA

DSB Task Force on Tactical Battlefield Communication

4001 North Fairfax Dr. Arlington, Va.

8 October 1999

TIME	
8:00	Task Force Informal Discussion (Coffee/Tea)
8:30	Task Force Discussion on Final Report and Out Brief Slides
10:30	BREAK
10:45	Task Force Discussion on Final Report and Out Brief Slides
12:00	ADJOURN

ANNEX D

JTRS INTERIM REPORT

The Defense Science Board

Task Force

Tactical Battlefield Communications

Interim Report on the
Joint Tactical Radio System Program

January 1999

Office of the Under Secretary of Defense
for Acquisition and Technology
Washington, DC 20301-3140

6 January 1999

Dr. Craig I. Fields
Chairman DSB, OUSD(A&T)
3140 Defense Pentagon, Room 3D965
Washington, DC 20301-3140

Dear Dr. Fields:

Attached is an interim report from the DSB Task Force on Tactical Battlefield Communications. At the request of our sponsors, the first meeting of the Task Force was dedicated to reviewing the Joint Tactical Radio System (JTRS) program. Due to time-sensitive issues associated with this extremely important initiative, the Task Force agreed to review the program status and provide its observations and recommendations on the JTRS within 30 days. To ensure that the Task Force members had the most recent perspectives on the program from the Office of the Secretary of Defense (OSD), military services, and contractors, an agenda was set that permitted each of these stakeholder communities to brief the Task Force members. This interim report presents our findings and recommendations on this program.

The Task Force members believe that the JTRS program could and should be a major turning point for achieving information superiority (IS) as envisioned in Joint Vision 2010 (JV2010). If the networking, bridging, routing, and automated system-management objectives called out in the JTRS Operational Requirements Document (ORD) are realized, the Services and DoD will have achieved the first and major component of a wireless common-user, quality-of-service (QoS)–based transport (communication) infrastructure that will

1. Meet many of the present Service communication needs that have been described to the Task Force
2. Provide a mechanism for integrating the many legacy, stovepipe, system-specific, point-to-point military radios into a single common-user framework
3. Provide the first truly Joint Information Transport Infrastructure, which is needed to support joint-service operations
4. Leverage commercial wireless transport technology—architecture, hardware and software
5. Lead to an open, scalable, flexible, wireless transport system that can grow as user needs and technology mature over time
6. Lead to decreased OSD ownership costs for the wireless transport infrastructure, as a result of the open, modular system design goals set in the ORD.

Furthermore, this potential can be realized much sooner than is currently envisioned by OSD and the Joint Program Office (JPO). By making JTRS available sooner to our military forces, we will minimize the continuing DoD investment in legacy stand-alone communication hardware and at the same time achieve a major step in establishing an integrated, joint, information infrastructure that is critical to future military operations.

To fully exploit this emerging opportunity, the Task Force has made a series of recommendations and presented them to our sponsors. These recommendations call for aggressively accelerating the acquisition of JTRS. A strategy is suggested to ensure that the system acquired is an open, flexible, scalable platform that leverages commercial digital telecommunication and networking technology to meet our military needs.

I would like to express my appreciation to the Task Force members who rose to the challenge of completing this report within the 30 day goal set for us. I would also like to thank the briefers who presented their views on the issues that we were addressing. We hope that our sponsors find the information contained in this interim report useful and the recommendations actionable.

Sincerely,

Dr. Michael S Frankel
Chairman, DSB Task Force on
Tactical Battlefield Communications

Attachment: *Interim Report on the Joint Tactical Radio System Program*

1. INTRODUCTION

On 19 and 20 November, the Defense Science Board Task Force on Tactical Communications convened its first meeting. The terms of reference (TOR) for this Task Force were approved by its three sponsors—USD/A&T, ASD/C3I and JCS/J6 during October 1998, and, signed by USD/A&T on 29 December 1998.* The TOR are provided in Appendix A.

At the request of our sponsors, the first meeting of the Task Force was dedicated to reviewing the Joint Tactical Radio System (JTRS) program. Due to time-sensitive issues associated with this extremely important initiative, the Task Force agreed to review the program status and provide its observations and recommendations on the JTRS within 30 days. To ensure that the Task Force members (Appendix B) had the most recent perspectives on the program from the Office of the Secretary of Defense (OSD), military services, and contractors, an agenda (Appendix C) was set that permitted each of these stakeholder communities to brief the Task Force members. The briefings were informative, and significant interaction occurred between the members and the briefers. The observations and recommendations that follow represent a Task Force consensus that resulted from our internal discussions during the 2-day meeting. An acronym glossary is furnished in Appendix D.

2. FINDINGS

The Task Force members believe that the JTRS program could and should be a major turning point for achieving information superiority (IS) as envisioned in Joint Vision 2010 (JV2010). If the networking, bridging, routing, and automated system-management objectives called out in the JTRS Operational Requirements Document (ORD) are realized, the Services and DoD will have achieved the first and major component of a wireless common-user, quality-of-service (QoS)–based transport (communication) infrastructure that will

1. Meet many of the present Service communication needs that have been described to the Task Force
2. Provide a mechanism for integrating the many legacy, stovepipe, system-specific, point-to-point military radios into a single common-user framework
3. Provide the first truly Joint Information Transport Infrastructure, which is needed to support joint-service operations
4. Leverage commercial wireless transport technology—architecture, hardware and software
5. Lead to an open, scalable, flexible, wireless transport system that can grow as user needs and technology mature
6. Lead to decreased OSD ownership costs for the wireless transport infrastructure as a result of the open, modular system design goals set in the ORD.

---

*USD/A&T: Under Secretary of Defense Acquisition and Technology; ASD/C3I: Assistant Secretary of Defense/Command, Control, Communications, and Intelligence; JCS/J6: Joint Chiefs of Staff/Joint Staff Command, Control, Communications, and Computers (C4) Systems Directorate.

The Task Force members were struck, in fact, by a sense that OSD and the Services did not appreciate the magnitude of the potential impact of the JTRS. The program name itself suggests that the DoD community is thinking of the program as buying a "radio" when in fact it is buying a "system" that will lead to a completely new form of communication infrastructure—one that supports such visions as Network Centric Warfare (J6); the Integrated Information Infrastructure (DSB); Navy 21; and The Infosphere (AF); as well as one that achieves the foundation assumption of information superiority in JV2010. JTRS is a really *Joint* Tactical Communication System (JTCS) that provides radios, routing/bridging services among legacy radio hardware, and future QoS-based transport services. The critical aspects of the system are not just the waveforms it supports, but the adaptive network and transport services it is required to provide.

The Service briefings tended to argue that the JTRS would be useful technology when delivered and if delivered at a competitive price. From the Service presentations and discussions, the Task Force noted the following:

1. The Army and Marine Corps support the program and its concepts. The Army's Near Term Digital Radio (NTDR) is a "today" version of the JTCS, wherein foundation technologies for JTRS are being demonstrated.

2. The Navy argued that it has a near-term need to consolidate several of its existing communications systems into a single box, the Digital Modular Radio (DMR). This approach provides the Navy with no significant increase in transport capability, does not provide network/bridging services, even among their own systems, and provides no support (other than what little exists with their legacy hardware) for joint military communications interoperability. The DMR is justified primarily by a near-term need to replace an aging set of Navy radio systems with a "today" hardware implementation of legacy communication services.

3. The Air Force argued that it too has platform and manpack radio needs that need near-term solutions. For the platform, aging equipment is again the key driver. The Task Force did not receive any information on the manpack requirements, but we are aware that a procurement has been put on hold by virtue of a draft Program Budget Decision (PBD) 290.

In the Service briefings, it was clear that each "dissenting" organization was basing its views on the "perceived" cost of, and the length of time until JTRS units would be available. Waivers to acquire legacy capabilities within the next 3 to 5 years were critical, primarily because of unsubstantiated arguments related to the increasing operations and maintenance (O&M) costs of communication hardware in the inventory today and "uncertainty" about JTRS— the Service representative did not discuss future requirements for transport capabilities and for Joint Service information exchange.

The private sector briefings were varied in viewpoint. However, the Task Force noted that in almost all cases the contractors understood the intent of the JTRS and its technical challenges. Several of the contractors argued that they foresaw a potential private-sector market for multiband, multimode, software-programmable radio systems similar to JTRS. The contractors

have been involved with the MMITS* forum, which is establishing a commercial, open, standards-based architectural framework for such a radio.

The Task Force members, based on the contractor briefings and the detailed experience of several members in developing JTRS-like systems, *see no technical show-stoppers* with respect to developing the JTRS. In fact, the Task Force feels that the JTRS can be put on *a much more aggressive acquisition cycle* than is presently envisioned by OSD and the Joint Program Office (JPO). The present strategy of "acquiring an architecture" first and then a brassboard JTRS in several years is much too modest a goal. We believe that prototypes that meet the general objectives of the ORD, realize the potential of the system as articulated above, adhere to the MMITS architectural framework, and provide the first set of open platforms *can be acquired in 12 to 14 months*.

By accelerating the acquisition of the Joint Tactical Communication System (JTCS),* with only modest risk, the Service goal to procure replacement hardware in the near term can be met, as well as the much broader and strategic objective of achieving a joint, wireless, common-user transport infrastructure. In addition to accelerating the acquisition process, the Task Force recommends that OSD clarify and/or consider modifying the following ORD needs as part of the prototype acquisition program.

1. The cost of the system will be significantly impacted by the number of legacy waveforms and crypto hardware the JTCS must support. The Task Force suggests that only a minimal, essential subset of military waveforms be acquired and supported by OSD and JPO. Two or three wideband legacy waveforms and several narrow-band legacy waveforms should be selected that maximize the integration of legacy systems into the common-user framework. Other waveforms deemed critical to the Services should be procured and maintained by them.

2. Compliance with the MMITS architectural framework, the JTA, and commercial open-system standards, practices and processes *must* continue to be heavily emphasized in the JTCS acquisition. System buses, well-defined APIs for software modules, and interface standards for all hardware modules must be, to the maximum extent possible, based on commercial standards. If no commercial standards are available, the specific JTCS interface specifications must be placed in the public domain.

3. Measures to ensure the modularity of software and hardware should emphasize ease of upgrading and of replacing functional components of the radio, both hardware and software. The goals to be achieved through the modular design include the following:

   A. Software changes to the fielded systems must be capable of being implemented via software upload into the radios. Furthermore, software

*MMITS: Mobile Modular Information Transfer System.

*The name JTCS will be used throughout this paper to emphasize the broader view of the program's objectives, as envisioned by the Panel.

uploads should not require the radios to be physically opened, or removed from the vehicles in which they may be mounted. Over the air, remote uploads should be the preferred mode of upgrading software or adding waveforms to the deployed system.

B. It must be possible to add and/or upgrade processors, memory, and the like in field units by changing or adding plug-in boards without removing the units from the platforms in which they may be installed.

C. As a result of this modularity, we fully expect that competition will be facilitated and will occur at the functional components of the system (e.g., hardware functional components such as RF units, modems, and general-purpose processes, and software functional components such as waveform software, Media Access Control (MAC) protocols, transport-level protocols, network, routing algorithms, and network management services).

4. Evolutionary increases in system capability should be expected. The system's modularity will permit the replacement of complete functional units within the platform as technology evolves over time. This type of evolution should permit the DoD to trade off *cost* between the *performance* and *delivery time* of a specific generation of the system. As technology matures, the growth of the platforms' capabilities incur minimal increases in unit costs.

   For example, broadband radio frequency power amplifiers that span 2–2500MHz and that can support several simultaneous broadband, complex waveforms are at the edge of today's technology (and consequently will be very expensive to design and produce). However, multiple, more narrow-band amplifiers can be obtained today that together can cover this entire frequency range. Using these amplifiers would result in a JTCS of much lower cost, delivered much sooner, than trying to build a JTCS based on a single broadband amplifier. In the future, though, as radio frequency power devices continue to evolve and become readily available in the marketplace, broadband power amplifiers will be available that could be placed into the JTCS as an upgrade to replace the various narrow-band units.

   A good analogy of this type of platform evolution, which should be the guiding model for the JTCS, is the desktop personal computer. These systems, using open standards and modularized in both hardware and software, are easily upgraded as new technologies evolve, e.g., x386 to x486 to Pentium IIs; replaceable video display cards that provide greater speed and display resolutions; replaceable modem cards that provide increased speed; and the like. Keeping this model in mind, the JTCS modularity does permit *time and cost to be truly independent variables* in its acquisition.

5. A stronger emphasis must be placed on developing future waveforms for DoD that will satisfy anticipated QoS and information-services needs. Several

emerging commercial wireless personal-communications (PCS) waveforms should also be supported on JTCS.

6. The JCTS network services—dynamic routing, self configuration packet-switching, QoS and the like—should be developed in compliance with JTA standards and, specifically, in compliance with present and evolving commercial Internet standards (IPV4, IPV6, Mobile IP). Furthermore, the JTCS should adhere to Internet naming and addressing conventions and be able to transport Internet packets as well as ATM cells.

7. More emphasis should be placed on a JTCS handheld unit in the ORD and in any future acquisition documents.

8. Much more analysis is required to define and specify a network security architecture for the JTCS. Over-the-air keying and rekeying; multilevel security; end-to-end security (vis-à-vis just transmission security); security support for highly mobile users as they cross virtual security domains; and the like are issues the Task Force did not hear discussed to any great depth. Such issues can make or break the JTCS unless carefully considered and addressed either technically, through CONOPS, or by a combination of both.

9. The JTCS should be viewed as providing transport-and-below services in the context of the OSI or DoD layered information system models. The ORD currently calls for the JTCS to provide message translation services, which is an application-layer gateway function. Burdening the JTCS with application services implies that all deployed JTCS units will have to be updated each time any service C4I-system PM makes a change to his or her message set data element (semantics) or message structure (syntax). In any well-engineered information technology (IT) system, applications and transport services are intentionally separated to minimize the impact of introducing new technologies and services at each layer. The same should hold true for the JTCS and more generally the evolving DoD Integrated Information Infrastructure.

The Task Force believes that one approach for OSD to accelerate JTCS fielding, and to motivate and test openness of the platform when it is delivered, is to acquire multiple JTCS prototype platforms within the next 12 to 14 months. The set of waveforms required for each prototype would include two legacy military wideband waveforms, two legacy military narrow-band waveforms, one commercial PCS waveform, and one *future* military *wideband waveform* (developed to supplier specifications). Each supplier should be asked to select a different set.

A midterm goal (i.e., to be achieved within a 6 month time frame) is to have all platform suppliers release their JTCS system architectures (APIs, interface specifications, and the like), and all waveform development tools, to the public domain. To test openness and interoperability, the government should then procure third-party hardware and software modules (waveforms) that meet the platform specification as a means of testing the platform's openness. Waveform compatibility should be tested against appropriate legacy radio hardware.

Each supplier should also be requested to host its waveforms on the other suppliers' platforms. This cross-supplier porting of waveforms will provide the government with an

assessment of how effective the waveform development tools are, how well each platform is specified through its system architecture, and how open the specifications are.

Finally, the government must establish an entity whose responsibilities will be to conduct systems engineering and architecture compliance evaluation and testing. This entity, comprising Service research and development staff as well as OSD leadership and guidance, should be tasked to provide system analysis, and testing and evaluation of each platform. The evaluation of system's compliance with the architectures, and of its openness, waveform interoperability, scalability, network services, and the like would be the basis for a down-selection of the prototype suppliers to a single supplier of production units. In addition, a JCS-led general office board of directors (with Service representatives at the lieutenant general level) should be established to monitor, facilitate, and support the JTCS initiative over the R&D phase of the program.

3. SUMMARY OF OBSERVATIONS

The JTCS has the potential to create a major point of inflection, in a highly positive sense, with respect to military operations, doctrine, organization, efficiency, and effectiveness. The reasons for this potential are somewhat complex, and transcend the basic rationale for the JTCS program, although they are closely related to the tactical objectives of the JTCS. The Task Force's observations are summarized as follows:

- The DoD has for many years sought to transcend its legacy of vertically structured information systems, without success. That thousands of such systems have been built to satisfy “stand-alone” requirements, from the technology, architectures, and acquisition methods of the moment, is well known and documented. No amount of expense or institutional energy has thus far been sufficient to overcome the interoperability issues associated with these myriad legacy systems; however, the technology necessary (and sufficiently developed) to satisfy the JTCS requirements, if fully exploited, has the potential to address the DoD legacy-system integration problems.

- The work done by DoD and the private sector on the Programmable Modular Communications System (PMCS), and the development of subsequent hardware and software systems, show unequivocally that digital waveform emulation in software is technically feasible. Moreover, this work proves that devices employing such capability can serve simultaneously both as translators between multiple RF systems and networks and as bridges between terrestrial RF, fiber-optic, cable and/or wire systems and airborne or space-based telecommunications (transport) systems.

- The functions of such devices can be readily changed through electronically distributed software. Present DoD and commercial technology can support multiple waveforms, security keys, network services such as ad hoc networking, dynamic routing, self organization, and self management.

- The current emphasis on recreating a radio architecture for the JTCS—and thus delaying the fielding of real capability—is not in the best interest of the DoD. Devices that incorporate the solutions to JTCS requirements, in addition to

addressing the broader field of digitally programmable multiband, multimode systems, have already been demonstrated; the technology is at hand to satisfy JTCS needs and similar needs throughout the civil and commercial sectors.

- The present strategy for arguing in favor of the JTCS puts system delivery beyond the near-term requirements for radio systems for which the AF and Navy are requesting waivers. However, accelerating the JTCS acquisition, with only modest risk, can meet the needs of the Services, thus obviating the need to buy more legacy hardware.

- There is a real danger that insistence on accommodating every legacy waveform in the military inventory will create, in the JTCS, merely another legacy system. At this juncture, it is reported that the JPO has been tasked with addressing some 37 different waveforms through the JTCS—substantially limiting the possibility of addressing future digital information transfer dynamics and, therefore, relegating the JTCS to the servicing of traditional analog telecommunications requirements. Such a limitation could indefinitely delay the effective application of digital information transfer capabilities to military operations, forcing the continuation of the present bandwidth-constrained legacy.

- It would appear that the substantial DoD investment already made in digital programmable communication systems—some $60,000,000 or so—has had little impact on JTCS program formulation or acquisition strategy. PMCS and several DoD programs such as Packet Radio[*], Global Mobile Information Systems (GloMo)[*] and Small Unit Operations (SUO)[*], consistent with the guidance of the Software Radio System (SRS) Forum [formerly the Mobile Modular Information Transfer System (MMITS) Forum], have validated network and hardware/software frameworks for wireless digital information-transfer systems. It is not necessary that the JPO conduct another architecture development. It is time to move on, get real hardware and software on the street, and seize the digital initiative, to the benefit of the nation's armed forces.

4. RECOMMENDATIONS

Consistent with the points made above, the following recommendations are offered for consideration by the sponsors of this study:

1. Instruct the JPO to stop, immediately, the ongoing JTRS architecture development procurement and to restructure its program so as to procure prototype JTCS platforms within 12 months (i.e., a request for proposal (RFP) should call for completion for a prototype system within 1 year of contract award). The prototypes should be based on the architecture developed under the SRS/MMITS Forum and the PMCS program. Upon completion of this

[*] All the programs are Defense Research Projects Agency (DARPA) advanced-technology initiatives

initial prototype system competition, a down-selection should be made for full production systems. This acquisition strategy is somewhat analogous to that of the Secure Telephone Unit III (STU-III) development effort.

2. Rename the Joint Tactical Radio System (JTRS) to be the Joint Tactical Communication System (JTCS) in order to raise awareness that an infrastructure is being procured, not a radio (box).

3. Restructure the direction provided to the JPO, so that emphasis is placed on the future rather than the past. Limit the number of legacy waveforms that the JTCS must address to those necessary to effect interoperability between *networks*, where necessary and appropriate, rather than between all legacy military radios. Relieve the JPO of the responsibility to satisfy all Service-unique waveform requirements. In those instances where the Services can unequivocally demonstrate a need to purchase legacy waveforms, allow the Service to fund the procurement at the absolute minimum level required to meet proven operational needs. The JPO should support only a few critical waveforms that maximize the interoperability and/or integration of service systems with a common-user information transport infrastructure.

4. Instruct the JPO to procure commercially developed PCS waveforms, such as the emerging W-CDMA* standards. The commercial industry is investing hundreds of millions of dollars for a spectrally efficient, high-data-rate-capable wireless system. The DoD could modify such a specification to operate within its licensed spectrum, imbedding the required security features and integrating additional services as needed.

5. Focus the JTCS effort on enabling new digital information system capabilities and services, such that the military services are motivated to help the program achieve its objectives rather than to seek waivers to permit the continuation of the legacy.

6. Deny requests for waivers to policy that would allow the continued acquisition of legacy radios, except where it can be proven that such waivers meet a critical short-term need that cannot be satisfied in the time available, even with an accelerated JTCS acquisition process.

7. Instruct the suppliers of the JTCS prototype platforms to put their system architectures and waveform development tools into the public domain within 6 months of contract award.

8. Expand the JPO's responsibilities to include system engineering (SE), standards compliance testing, platform openness evaluations, and waveform compatibility testing. Provide resources from the military research and development laboratories to support this JPO-led SE mission.

* W-CDMA: Wideband Code Division Multiple Access

9. Establish at the Lieutenant General level, a JPO Board of Directors (BoD), led by the J6 and having Service and OSD representatives, whose purpose would be to facilitate and ensure that it meets its *strategic* potential.

10. Direct JPO to establish an integrated security architecture and an associated time-phased implementation plan for the JTCS. The BoD should address and clarify security policy and CONOPS, while the JPO addresses the technical aspects of this architecture.

Appendix A

TERMS OF REFERENCE

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference for the Defense Science Board Task Force on Tactical Battlefield Communications

You are requested to form a Defense Science Board (DSB) task Force on Tactical Battlefield Communications to determine U.S. needs for wireless communications on future battlefields and the adequacy of communication architecture plans to fulfill those needs. You should specifically address the ability of digital and analog communications below the Corps-level to support predicted demands of joint tactical, intelligence, logistics and medical actions while assuring combatants' effectiveness and safety.

Tasks to be Accomplished:

The Tactical Battlefield Communications Task Force will provide advice, recommendations, and supporting rationale that address the items below for OSD, the Military Departments, the Joint Staff, Unified and Specified Combat Commands and the Defense Agencies:

-- Adequacy of forecasted tactical communications requirements for evolving concepts such as Army After 2010, Operational Maneuver from the Sea, Air Expeditionary Force and Extended Littoral Battlespace. Interoperability requirements to support joint operations, should also be reviewed.

-- Adequacy of DOD communication vision and architectures capable of meeting forecasted service and joint requirements.

-- Adequacy of companion communication security architecture to assure force protection and information assurance.

-- Funding and capitalization constraints that restrict ability to make the transition from equipment in the current inventory to equipment needed to meet the evolving communications requirements.

-- Adequacy of tactical communications equipment now in the DOD inventory, or under development, to fulfill the evolving communications requirements, to include; operational experience with communications equipment in ATDs and ACTDs.

-- Adequacy of acquisition strategy and policy to meet evolving communication architectures and requirements that facilitates exploiting of commercial and DOD-developed technologies and services.

The Task Force should provide specific advice for addressing its findings.

The study will be co-sponsored by the Under Secretary of Defense (Acquisition and Technology) and the Senior Civilian Official, OASD (C3I) and the Director, JCS(J-6). Dr. Michael Frankel will serve as the Task Force Chairman. Mr. Bennett Hart, OASD/C3I, will serve as the Executive Secretary and Maj Tony Yang, USAF, will serve as the Defense Science Board Secretariat Representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DOD Directive 5104.5 "DOD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.

//signed//

J.S. Gansler

Appendix B

TASK FORCE MEMBERS

Defense Science Board
Task Force
on
Tactical Battlefield Communications

1.1 MEMBERS

Dr. Mike Frankel [*] (Chair)
SRI International

Dr. Reza Eftakari
The MITRE Corp.

Dr. William H. Evers Jr.
Systems Technology and Science

Dr. William G Howard *
Consultant

Dr. Gary Minden
University of Kansas

Mr. Stu Personick
Drexel University

Mr. Mark Rich
SRI International

Dr. Scott Snyder
Lockheed Martin Telecommunications (LMT)

Mr. Peter D. Steensma
ITT Aerospace/Communications

Mr. John Stenbit*
TRW Systems Integration Group

Mr. Owen Wormser
C3I

Mr. Bennett Hart (Executive Secretary)
OASD(C4I)

*** DSB member**

ADVISORS

CAPT Gary Grauptmann, USN

Mr. Dave Keetley
CECOM

Col Dan Ryan, USA
OJCS/J6

Mr. Vic Russell
OASD(C4I)

Col Bobby Smart, USAF

SUPPORT

Maj Tony Yang, USAF
DSB Secretariat

Ms. Donna Preski
SAIC

Col George M. Mcveigh, USAF (RET)
SAIC

[*]DSB member.

Appendix C

AGENDA

Agenda

DSB Task Force on Tactical Battlefield Communications

November 19, 1998

7:30	**Coffee/Tea**
8:15	**Task Force Administration**
	Mr. George McVeigh, SAIC
8:30	**General Counsel Handout**
	Members
8:45	**Chairmen's Opening Remarks**
	Dr. Mike Frankel
9:15	**Study Plan**
	Dr. Mike Frankel
9:45	**Break**

OSD PERSPECTIVE

10:00 **Joint Tactical Radio System (JTRS) Background/History**

Mr. Vic Russell, OASD(C^3I)

10:15 **Joint Requirements /Army Requirements**

Col James Schroeder, Army TRADOC Systems Manager

11:30 **Program Overview and Status**

Col Tony Badolato, JTRS Program Manager

12:00 **Lunch**

SERVICES PERSPECTIVES

EXISTING PROGRAMS AND PROPOSED JTRS MIGRATION PLANS

12:30 **Navy Requirements**

CAPT Gary Graupmann, Navy PM DMR

1:30 **Air Force Requirements**

Maj Eric Bellows, AC2A/C2G, and Maj James Forney, ESC/DIG

2:30 **Break**

2:45 **Marine Corp Requirements**

Col Robert Logan, Director Requirements Division, Combat Development

3:45 **Discussion**

5:00 **Adjourn**

Agenda

DSB Task Force on Tactical Battlefield Communications

November 20, 1998

7:30	**Coffee/Tea**

PRIVATE SECTOR PERSPECTIVES

(open standards, line level vs. box competition, etc.)

8:00	**Motorola – DMR** *Mr. Mike Lyga*
9:00	**ITT –NTDR** *Mr. Ed Dauksz,*
10:00	**Break**
10:15	Raytheon – DMR, JTT, AITG *Bill Langford*
11:15	Open Systems Study Briefing *Mr. Chris Waln, TASC*
12:15	**Lunch**
12:45	**Rockwell – ARC-210/DCS-2000**
13:45	**Member Discussions** *Members and Advisors*
3:30	**Adjourn**

Appendix D

GLOSSARY

Glossary

AF	Air Force
API	Applications Program Interface
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
ATM	Asynchronous Transfer Mode
C3I	Command, Control, Communications and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CONOPS	Concept of Operations
DARPA	Defense Advance Research Development Agency
DMR	Digital Modular Radio
DoD	Department of Defense
DSB	Defense Science Board
GloMo	Global Mobile Information Systems
IS	Information Superiority
IT	Information Technology
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
JCS	Joint Chiefs of Staff
JPO	Joint Program Office
JTA	Joint Technical Architecture
JTCS	Joint Tactical Communications System
JTRS	Joint Tactical Radio System
JV2010	Joint Vision 2010
MAC	Media Access Control
MMITS	Mobile Modular Information Transfer System
Mobile IP	Mobile Internet Protocol
NTDR	Near Term Digital Radio
O&M	Operations and Maintenance
ORD	Operational Requirements Document

OSD	Office of the Secretary of Defense
PBD	Program Budget Decision
PCS	Personal Communication System
PM	Program Manager
PMCS	Programmable Modular Communications System
QoS	Quality of Service
R&D	Research and Development
RF	Radio Frequency
RFP	Request for Proposal
SE	Systems Engineering
SRS	Software Radio System
STU-II	Secure Telephone Unit-III
SUO	Small Unit Operations
TOR	Terms of Reference
USD (A&T)	Under Secretary of Defense Acquisition and Technology
W-CDMA	Wideband Code-Division Multiple Access

ANNEX E

ACRONYMS

AAN	Army After Next
AAV	Autonomous Air Vehicles
ACAT	Acquisition Category
ACC	Architecture Coordination Council
ACN	Airborne Communication Node
ACN	Airborne Communication Node
ACTD	Advanced Concept Technology Demonstration
ADM	Add/Drop Multiplexers
AEF	Air Expeditionary Force
AFSAB	Air Force Science Advisory Board
AMPS	Advanced Mobile Phone Service
API	Application Program Interface
ASD/C3I	Assistant Secretary of Defense for Command, Control and Communications
ATD	Advanced Technical Demonstrations
ATM	Asynchronous Transfer Mode
AWE	Advanced Warfighting Experiment
BoD	Board of Directors
bps	bits per second
C2	Command and Control
C3I	Command, control, communications, and intelligence
C4ISR	Command, control, communications, computers, intelligence, surveillance, and reconnaissance
C4RDP	Command, control, communications, computers, requirements definition program
CAP	Common Air Picture
CDPD	Cellular Digital Packet Data
CDSA	Common Data Security Architecture
CEC	Cooperative Engagement Capabilities
CECOM	U.S. Army Communications Electronics Command
CGP	Common Ground Picture

CINC	Commander in Chief
CIO	Chief Information Officer
CIO	Chief Information Officer
CMA	Collection Management Authority
CMP	Common Maritime Picture
COMSEC	Communication Security
CONUS	Continental United States
COP	Common Operational Picture
CRD	Capstone Requirements Document
CSCI	Commercial Satellite Communications Initiative
CWAN	Coalition Wide Area Network
DARPA	Defense Advanced Research Projects Agency
DDR&E	Director Defense Research and Engineering
DES	Data Encryption Standard
DISN	Defense Information Systems Network
DoD	Department of Defense
DSB	Defense Science Board
DSC	Decision Support Center
DSCS	Defense Satellite Communications System
DSCS	Defense Satellite Communications System
DSTS-G	DISN Satellite Transmission Services - Global
DWDM	Dense Wave Division Multiplexing
EFX	Ecpeditionary Force Experiment
ELB	Extended Littoral Battlespace
ESC	Electronic Systems Command
FTX	Field Training Exercises
GEO	Geostationary Earth Orbiting
GIG	Global Information Grid
GloMo	Global Mobile
GNIE	Global Networked Information Enterprise
HALE	High Altitude Long Enduring

IA	Information Assurance
IC	Intelligence Community
ICAP	Integrated Communications Access Package
ID/IQ	Indefinite Delivery/Indefinite Quality
IDC	International Data Corporation
IER	Information Exchange Requirements
IETF	Internet Engineering Task Force
III	Integrated Information Infrastructure
InfoSec	Information Security
IOC	Initial Operational Capability
IP	Internet Protocol
IPSec	Internet Protocol security
ISR	Intelligence, Surveillance and Reconnaissance
ISX	Information Superiority Experiment
IT	Information Technology
ITEF	Internet Engineering Task Force
JCS	Joint Chiefs of Staff
JIER	Joint Information Exchange Requirements
JOA	Joint Operational Architecture
JROC	Joint Requirements Oversight Council
JSA	Joint System Architecture
JSMB	Joint Space Management Board
JSTARS	Joint Surveillance Target Attack Radar System
JTA	Joint Technical Architecture
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
JV 2010	Joint Vision 2010
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Networks
LEO	Low Earth Orbiting

LTM	Last Tactical Mile
M&S	Modeling and Simulation
MCEB	Military Communications Electronics Board
MEO	Mid Earth Orbiting
MilSatCom	Military Satellite Communications
MOS	Military Operations Specialties
MRC	Major Regional Conflict
MTW	Major Theaters of War
MUOS	Mobile Users Objective System
NAD	Naval Architecture Database
NAN	Navy After Next
NCW	Network Centric Warfare
NED	Network Encryption Devices
NETWARS	Network Warfare Simulation
NGI	Next Generation Internet
NIPRNET	Non Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NRE	Non-Recurring Engineering
NRO	National Reconnaissance Office
NSA	National Security Agency
NSB	Naval Studies Board
NSSN	Next Subsurface Nuclear (submarine)
O&M	Operation and Maintenance
OA	Operational Architecture
OASD/C3I	Office of the Assistant Secretary of Defense, Command, Control, Communications & Intelligence
OMFTS	Operational Maneuver from the Sea
OPFAC	Operations Facility
OPNET	Operations Network
ORD	Operational Requierments Document
OSD	Office of the Secretary of Defense

PCS	Personal Communications Systems
PDA	Personal Digital Assistants
PEO	Program Executive Office
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PM	Program Manager
POM	Program Objective Memorandum
QoS	Quality-of-service
RSVP	Resource Reservation Protocol
RTP	Real-Time Protocol
S&T	Science and Technology
SA	System Architecture
SAM	Surface to Air Missile
SatCom	Satellite Communications
SDR	Surrogate Digital Radio
SINCGARS	Single Channel Ground and Airborne Radio System
SIPRNET	Secure Internet Protocol Router Network
SLEP	Service Life Enhancement Program
SSG	Senior Steering Group
SSL	Secure Socket Layer
SSNMP	Secure Simple Network Management Protocol
STEP	Standardized Tactical Entry Point
SUO	Small Unit Operations
TA	Technical Architecture
TADIL J	tactical digital information link, type J (JTIDS)
TDC	Theater Deployable Communications
TIARA	Tactical Intelligence and Related Activities
TOR	Terms of Reference
TRANSEC	Transmission Security
UAV	Unmanned Aerial Vehicle
UFO	UHF Follow-On Satellite System

UHF	Ultra High Frequency
USD/AT&L	Under Secretary of Defense for Acquisition, Technology and Logistics
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconferencing
WIN-T	Warfighter Information Network-Tactical
WMD	Weapon of Mass Destruction